# Table of Contents

## About This Guide
- Overview                           xi
- Target Audience                    xi
- Conventions
  - Headings                           xii
  - Typeface                           xii
  - Cross References                   xii
  - Messages                           xii
- Product Documentation              xiii
- Customer Support                   xiii
  - Contact Information                xiv

## System Overview
- Overview                           1
- TippingPoint Architecture          2
- Security Management System (SMS)   2
  - SMS Server                        3
  - SMS Client                        3
- Intrusion Prevention System Devices (IPS)
  - IPS Local Clients                 5
- Core Controller                    5
- High Availability                  6
- Threat Suppression Engine          6
- Threat Management Center           7

## IPS Concepts and the LSM
- Overview                           9
- IPS Deployment                     10
- Threat Suppression Engine          10
- IPS Filtering
  - The Digital Vaccine Package       11
  - Filter Components                 11
  - Categories and Category Settings  12
  - Filter Override Settings          12
  - Filter Limits and Exceptions      13
  - Adaptive Filtering                13
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS/NMS</td>
<td>106</td>
</tr>
<tr>
<td>Configure SMS Information</td>
<td>107</td>
</tr>
<tr>
<td>View or Configure NMS Information</td>
<td>107</td>
</tr>
<tr>
<td>Disable/Enable SMS Management</td>
<td>108</td>
</tr>
<tr>
<td>High Availability</td>
<td>108</td>
</tr>
<tr>
<td>Configuring High Availability from the LSM</td>
<td>109</td>
</tr>
<tr>
<td>Compact Flash</td>
<td>109</td>
</tr>
<tr>
<td>Thresholds</td>
<td>110</td>
</tr>
<tr>
<td>Set disk usage and memory thresholds</td>
<td>110</td>
</tr>
<tr>
<td>Email Server</td>
<td>111</td>
</tr>
<tr>
<td>Email Threshold</td>
<td>111</td>
</tr>
<tr>
<td>Testing Email</td>
<td>111</td>
</tr>
<tr>
<td>Syslog Servers</td>
<td>112</td>
</tr>
<tr>
<td>Named Networks</td>
<td>112</td>
</tr>
<tr>
<td>Adding a Named Network</td>
<td>113</td>
</tr>
<tr>
<td>License</td>
<td>114</td>
</tr>
<tr>
<td>Network</td>
<td>115</td>
</tr>
<tr>
<td>Overview</td>
<td>115</td>
</tr>
<tr>
<td>Segments</td>
<td>116</td>
</tr>
<tr>
<td>Edit IPS Segment Page</td>
<td>117</td>
</tr>
<tr>
<td>Configure a Segment</td>
<td>118</td>
</tr>
<tr>
<td>Network Ports</td>
<td>118</td>
</tr>
<tr>
<td>Edit Port Configuration</td>
<td>120</td>
</tr>
<tr>
<td>Click <strong>Apply</strong> to save the configuration and restart the port.</td>
<td>120</td>
</tr>
<tr>
<td>Disable a Port</td>
<td>120</td>
</tr>
<tr>
<td>Restart a Port</td>
<td>120</td>
</tr>
<tr>
<td>Correcting Port Link-Down Errors</td>
<td>121</td>
</tr>
<tr>
<td>Virtual Ports</td>
<td>121</td>
</tr>
<tr>
<td>Virtual Port Example</td>
<td>122</td>
</tr>
<tr>
<td>Configuration Overview: Ports and Segments</td>
<td>123</td>
</tr>
<tr>
<td>Create a Virtual Port</td>
<td>123</td>
</tr>
<tr>
<td>Edit a Virtual Port</td>
<td>124</td>
</tr>
<tr>
<td>Virtual Segments</td>
<td>124</td>
</tr>
<tr>
<td>Create a Virtual Segment</td>
<td>125</td>
</tr>
<tr>
<td>Delete a Virtual Segment</td>
<td>125</td>
</tr>
<tr>
<td>VLAN Translation</td>
<td>126</td>
</tr>
<tr>
<td>Create a VLAN Translation</td>
<td>127</td>
</tr>
<tr>
<td>Network Tools</td>
<td>128</td>
</tr>
<tr>
<td>Starting a Traffic Capture</td>
<td>129</td>
</tr>
<tr>
<td>Traffic Capture Expressions</td>
<td>129</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>TPT-RESOURCE</td>
<td>157</td>
</tr>
<tr>
<td>TPT-SMSMIBS</td>
<td>157</td>
</tr>
<tr>
<td>TPT-SMS-TRAP-MIB</td>
<td>157</td>
</tr>
<tr>
<td>TPT-TPA-HARDWARE</td>
<td>157</td>
</tr>
<tr>
<td>TPT-TPAMIBS</td>
<td>157</td>
</tr>
<tr>
<td>TPT-TRAFFIC</td>
<td>157</td>
</tr>
<tr>
<td>TPT-TSE</td>
<td>157</td>
</tr>
<tr>
<td>Using HP OpenView With IPS MIBs</td>
<td>158</td>
</tr>
<tr>
<td>Loading TippingPoint Enterprise MIBs</td>
<td>158</td>
</tr>
<tr>
<td>MIB Application Builder</td>
<td>158</td>
</tr>
<tr>
<td>Discovering the IPS</td>
<td>159</td>
</tr>
<tr>
<td>Creating Graphs with Application Builder</td>
<td>160</td>
</tr>
</tbody>
</table>

**Glossary** | 161

**Index**     | 171
List of Figures

<table>
<thead>
<tr>
<th>Figure Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TippingPoint Architecture</td>
<td>2</td>
</tr>
<tr>
<td>IPS Deployment Example</td>
<td>10</td>
</tr>
<tr>
<td>LSM Logon Page</td>
<td>16</td>
</tr>
<tr>
<td>LSM Screen Layout</td>
<td>17</td>
</tr>
<tr>
<td>Filters Page with Search</td>
<td>30</td>
</tr>
<tr>
<td>Edit Security Profile Page - Category Settings</td>
<td>35</td>
</tr>
<tr>
<td>Network with VLAN Translation</td>
<td>126</td>
</tr>
</tbody>
</table>
List of Tables

Main Menu Bar Options 18
Navigation Options 18
Security Profile Details 25
Port Configuration 26
Sample Security Profiles 26
Sample Security Profile Zone Configuration 27
Sample Security Profile Zone Configuration 27
Sample Security Profile Zone Configuration 28
Search Filter Criteria Parameters 31
Filter List Details 32
Traffic Management Profile Details 41
IP Filter Settings 43
Traffic Management Filter 45
Security Profile Details 47
Action Sets 51
Action Sets Details 51
Contacts List 54
IPS: IPS Services Details 58
IPS Preferences: TSE Configuration Parameters 60
Alert Log Field Descriptions 65
Block Log Field Descriptions 66
Audit Log Field Descriptions 67
System Log Field Descriptions 68
Log Functions 69
Blocked Streams Table 73
Rate Limited Streams Table 75
Quarantined Address(es) Table 77
Trusted Streams Table 79
Device Health 81
Performance/Throughput 82
<table>
<thead>
<tr>
<th>Table Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Health</td>
<td>83</td>
</tr>
<tr>
<td>TSE Adaptive Filter Configuration Details</td>
<td>89</td>
</tr>
<tr>
<td>LSM Management Port Configuration Options</td>
<td>101</td>
</tr>
<tr>
<td>High Availability Details</td>
<td>108</td>
</tr>
<tr>
<td>Named Network features</td>
<td>113</td>
</tr>
<tr>
<td>License Status</td>
<td>114</td>
</tr>
<tr>
<td>Segment Configuration Parameters</td>
<td>117</td>
</tr>
<tr>
<td>Port Configuration Parameters</td>
<td>119</td>
</tr>
<tr>
<td>Virtual Port Configuration Parameters</td>
<td>122</td>
</tr>
<tr>
<td>Virtual Segment Configuration Parameters</td>
<td>125</td>
</tr>
<tr>
<td>VLAN Translations Parameters</td>
<td>127</td>
</tr>
<tr>
<td>VLAN Translations Table</td>
<td>127</td>
</tr>
<tr>
<td>Traffic Capture Parameters</td>
<td>128</td>
</tr>
<tr>
<td>Traffic Capture Table</td>
<td>128</td>
</tr>
<tr>
<td>LSM Functions available to TOS Users based on Access Level</td>
<td>133</td>
</tr>
<tr>
<td>Login and Password Name Examples</td>
<td>134</td>
</tr>
<tr>
<td>Authentication: General User Preferences</td>
<td>136</td>
</tr>
<tr>
<td>Authentication: TOS User Preferences</td>
<td>136</td>
</tr>
<tr>
<td>Alert and Block Log Formats</td>
<td>146</td>
</tr>
<tr>
<td>Audit Log Format</td>
<td>148</td>
</tr>
<tr>
<td>System Log Format</td>
<td>149</td>
</tr>
<tr>
<td>Remote Syslog Field Descriptions</td>
<td>150</td>
</tr>
<tr>
<td>High Availability Log Messages</td>
<td>151</td>
</tr>
<tr>
<td>IPS Update States</td>
<td>152</td>
</tr>
<tr>
<td>IPS Update Failure Messages</td>
<td>152</td>
</tr>
<tr>
<td>Virtual Port</td>
<td>168</td>
</tr>
</tbody>
</table>
About This Guide

Explains intended audience, where related information is located, and how to obtain customer support.

Overview

Welcome to the TippingPoint Local Security Manager User's Guide.

This section includes the following items:

- “Target Audience” on page xi
- “Conventions” on page xii
- “Product Documentation” on page xiii
- “Customer Support” on page xiii

Target Audience

The intended audience includes technicians and maintenance personnel responsible for installing, configuring, and maintaining TippingPoint security systems and associated devices. Users should be familiar with networking concepts and the following standards and protocols:

- TCP/IP
- UDP
- ICMP
- Ethernet
- Simple Network Time Protocol (SNTP)
- Simple Mail Transport Protocol (SMTP)
- Simple Network Management Protocol (SNMP)
Conventions

The TippingPoint documentation uses the following conventions for structuring information.

Headings

Each main section starts with a brief description of the information you can find in that section, which correlates with the major headings in that section. Each major heading corresponds to a task or concept that is important for you to understand. Headings are of a different size and type to make them easy to skim, whether you are viewing an online or print copy of this document.

Typeface

This document uses the following typeface conventions:

- **Bold**: Used for the names of screen elements like buttons, drop-down lists, or fields. For example, when you are done with a dialog, you would click the **OK** button.
- **Code**: Used for text a user must type to use the product.
- **Italic**: Used for book titles, variables, and important terms.
- **Hyperlink**: Used for Web site and cross reference links.

Cross References

When a topic is covered in depth elsewhere in this document, or in another document in this series, a cross reference to the other information is provided as follows:

Messages

Messages are emphasized by font, format, and icons. There are four types of messages in this document:

- **Warnings**: indicate how to avoid physical injury to people or equipment. For people, injury includes anything from temporary conditions, such as pain, to irreversible conditions such as death. For equipment, injury includes anything requiring repair. Warnings indicate what you should or should not do and the consequences of not heeding the warning.
- **Cautions**: indicate how to avoid a serious loss that stops short of physical damage, such as the loss of data, time, or security. Cautions indicate what you should or should not do to avoid such losses and the consequences of not heeding the caution.
- **Notes**: Notes indicate information that might not be obvious or that does not relate directly to the current topic, but that may affect relevant behavior.
- **Tips**: Tips are suggestions about how to perform a task more easily or more efficiently.
Warning

Warnings are represented by a red octagon with a white lightning bolt drawn inside. Warnings also start with the word “WARNING” and are presented in bold face type.

**WARNING:** Only trained and qualified personnel should install, replace, or service this equipment. Disconnect the system before servicing.

Caution

Cautions are represented by a yellow triangle icon with a black exclamation point drawn inside. Cautions also start with the word “CAUTION”.

**CAUTION:** Do not type `del *./*` from the root (C:\) directory. Typing `del *./*` from the root directory will destroy all the program and configuration data that your computer needs to run, and will render your system inoperable.

Note

A note has an icon represented by a piece of note paper and starts with the word “Note”.

**Note:** To view information about attacks, you must have Operator authority. To create or edit attack filters and related objects, you must have Super User or Administrator authority.

Tip

A tip is represented by a circle icon with a light bulb drawn inside and starts with the word “Tip”.

**Tip:** Setting the logging parameter to “off” or “minimal” will improve your system’s processing performance, but it will make debugging very difficult in the event of a system crash. During system integration, you can set logging to “full” to ease debugging. After you have finished testing, set logging to “minimal” to improve performance.

Product Documentation

TippingPoint Systems have a full set of documentation. For the most current documentation, check the Threat Management Center (TMC) Web site at [https://tmc.tippingpoint.com](https://tmc.tippingpoint.com).

Customer Support

TippingPoint is committed to providing quality customer support to all of its customers. Each customer is provided with a customized support agreement that provides detailed customer and support contact information.
For the most efficient resolution of your problem, take a moment to gather some basic information from your records and from your system before contacting customer support, including your customer number.

Have the following information available:

<table>
<thead>
<tr>
<th>Information</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer number</td>
<td>You can find this number on your Customer Support Agreement and on the shipping invoice that came with your TippingPoint system.</td>
</tr>
<tr>
<td>Device serial number</td>
<td>You can find this information on the bottom of the server chassis. Also, from the CLI, you can run the <code>show version</code> command.</td>
</tr>
<tr>
<td>Device version number</td>
<td>From the CLI, you can run the <code>show version</code> command.</td>
</tr>
</tbody>
</table>

**Contact Information**

Use the following information to contact TippingPoint Customer Support:

For additional information or assistance, contact TippingPoint Customer Support:

**Telephone**

**North America:** +1 866 681 8324  
**International:** +1 512 681 8324

For a list of international toll-free contact numbers, consult one of the following web pages:

- [https://tmc.tippingpoint.com/TMC/Content/support/Support_Contacts](https://tmc.tippingpoint.com/TMC/Content/support/Support_Contacts)  
- [http://www.tippingpoint.com/support.html](http://www.tippingpoint.com/support.html)

**E-mail**

support@tippingpoint.com
System Overview

The TippingPoint™ system is a security suite of products and software that includes the Intrusion Prevention System (IPS), Local Security Manager (LSM), Digital Vaccine™, the Security Management System Appliance™, and the Core Controller.

Overview

Enterprise security schemes once consisted of a conglomeration of disparate, static devices from multiple vendors. Today, TippingPoint’s security system provides the advantages of a single, integrated, highly adaptive security system that includes powerful hardware and an intuitive management interface.

This section includes the following topics:

- “TippingPoint Architecture” on page 2
- “Security Management System (SMS)” on page 2
- “Intrusion Prevention System Devices (IPS)” on page 4
- “Core Controller” on page 5
- “High Availability” on page 6
- “Threat Suppression Engine” on page 6
- “Threat Management Center” on page 7
TippingPoint Architecture

The TippingPoint System uses a flexible architecture that consists of a Java-based SMS Client, SMS Management Server, IPS device(s), and Local Clients including the Local Security Manager (LSM) and Command Line Interface (CLI). The system may also include the Core Controller, a hardware appliance that balances traffic loads for one or more IPSes. The following diagram provides an overview of the architecture:

Figure 1 - 1: TippingPoint Architecture

Security Management System (SMS)

The SMS core components include:

- **SMS Secure Server** — hardware appliance for managing multiple devices
  - SMS Home Page — web-based interface with links to current Client software, documentation, and the Threat Management Center
- **SMS Management Client** — Java-based application for Windows or Linux workstations used to manage your TippingPoint system
  - Graphical User Interface (GUI)
  - Dashboard
  - Command Line Interface (CLI)

The SMS communicates with managed devices that are installed in your network.
The SMS architecture also includes the following components:

- **Threat Management Center** (TMC) — Centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation.
- **Digital Vaccine** (DV) — Update service that includes up-to-date filter packages for protecting your network
- **Managed Devices** — TippingPoint IPS or Core Controller devices that are installed in your network

**SMS Server**

The SMS Server is an enterprise-class management platform that provides centralized administration, configuration, monitoring and reporting for well over a hundred TippingPoint IPS devices. The SMS provides the following functionality:

- **Enterprise-wide device status and behavior monitoring** — Stores logs and device status information, manages updates, and monitors filter, device, software, and network status.
- **IPS networking and configuration** — Stores device information and configures devices according to the settings that are modified, imported, or distributed by clients. These settings affect the flow and detection of traffic according to device, segment, or segment group.
- **Filter customization** — Stores filter customizations in profiles as maintained by the SMS client. These settings are distributed and imported to devices, which can be reviewed and modified by local clients. If a device is managed by the SMS Server, the local clients cannot modify settings.
- **Filter and software distribution** — Monitors and maintains the distribution and import of filters, Digital Vaccine packages, and software for the TippingPoint Operating System and SMS Client. The SMS client and Central Management Server can distribute these packages according to segment group settings. The Central Management Server maintains a link to the Threat Management Center (TMC) for downloading and installing package updates.

**SMS Client**

The TippingPoint Security Management System (SMS) client provides services and functions to monitor, manage, and configure the entire TippingPoint system. This client is a Java-based application installed and accessed on a computer running the appropriate operating system. Each user receives a specific user level with enhanced security measures to protect access and configuration of the system.
You can monitor the entire TippingPoint system through the SMS client on a computer with the following requirements:

- One of the following operating systems:
  - Windows 98, 2nd edition
  - Windows NT, Service Pack 5 or later
  - Windows 2000, Service Pack 3 or later
  - Windows XP
  - Apple
  - Red Hat Linux
- One of the following browsers:
  - Microsoft Internet Explorer, version 6.0 or higher
  - Firefox
  - Safari

The SMS features a policy-based operational model for scalable and uniform enterprise management. It enables behavior and performance analysis with trending reports, correlation and real-time graphs — including reports on all, specific, and top attacks and their sources and destinations as well as all, specific, and top peers and filters for misuse and abuse (peer-to-peer piracy) attacks. You can create, save, and schedule reports using report templates. All reports are run against system and audit logs stored for each device managed by the system. These logs detail triggered filters. You can modify, update, and control distribution of these filters according to segment groups for refined intrusion prevention.

The SMS dashboard provides at-a-glance monitors, with launch capabilities into the targeted management applications that provide global command and control of TippingPoint. It displays the entries for the top 5 filters triggered over the past hour in various categories, a graph of triggered filters over the past 24 hours, the health status of devices, and update versions for software of the system. Through the Dashboard, you gain an overview of the current performance of your system, including notifications of updates and possible issues with devices monitored by the SMS.

**Intrusion Prevention System Devices (IPS)**

Intrusion Prevention System (IPS) devices protect your network with the Threat Suppression Engine (TSE) by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device by a client.

Each device provides intrusion prevention for your network according to the number of network connections and hardware capabilities. IPS devices also have built-in intrinsic high-availability features, guaranteeing that the network keeps running in the event of system failure.

TippingPoint Intrusion Prevention Systems are optimized to provide high resiliency, high availability security for remote branch offices, small-to-medium and large enterprises and collocation facilities. Each TippingPoint can protect network segments from both external and internal attacks.
IPS devices provide the following segments and traffic performance:

- TippingPoint 200/200E — Two 10/100 segments, 200 megabits/second
- TippingPoint 210E — Five 10/100/1000 segments, 200 megabits/second
- TippingPoint 400 — Four 10/100 segments, 400 megabits/second
- TippingPoint 600E — Four 10/10/1000 segments, 600 megabits/second
- TippingPoint 1200/1200E — Four 10/100/1000 segments, 1.2 gigabits/second
- TippingPoint 2400/2400E — Four 10/100/1000 segments, 2.0 gigabits/second
- TippingPoint 5000E — Four 10/100/1000 segments, 5.0 gigabits/second
- TippingPoint 660N — 600 megabits/second
- TippingPoint 1400N — 1 gigabit/second
- TippingPoint 2500N — Five 1GbE copper segments, five 1GbE fiber segments, and one 10GbE fiber segment, 2.0 gigabits/second
- TippingPoint 5100N — Five 1GbE copper segments, five 1GbE fiber segments, and one 10GbE fiber segment, 5.0 gigabits/second

Multiple TippingPoint devices can be deployed to extend this unsurpassed protection to hundreds of enterprise zones. You can monitor and manage the devices by using the local client available on each device, or by using the SMS client to monitor and manage well over a hundred devices. E-Series systems provide Advanced DDoS protection. The TippingPoint N-Series support IPv6, tunneling (including GRE and multi-layer tunnels), and inspection bypass rules for trusted traffic.

**IPS Local Clients**

The TippingPoint System provides various points of interaction, management, and configuration of the intrusion prevention system. The clients include graphical user interfaces (GUI) and command line interfaces (CLI). These clients include the following:

- **Local Security Manager (LSM)** — Web-based GUI for managing one IPS device. The LSM provides HTTP and HTTPS (secure management) access. This access requires access from a supported web browser (Internet Explorer, Mozilla Firefox, and Netscape). Using the LSM, you have a graphical display for reviewing, searching, and modifying settings. The GUI interface also provides reports to monitor the device traffic, triggered filters, and packet statistics.
- **Command Line Interface (CLI)** — Command line interface for reviewing and modifying settings on the device. The CLI is accessible through Telnet, SSH (secure access), and the Console serial port.
- **LCD Panel** — Several IPS TippingPoint devices provide an LCD panel to view, configure and modify some device settings.

**Core Controller**

The TippingPoint Core Controller is a hardware-based device that enables inspection of up to 20 Gbps of traffic by sending the traffic to as many as 24 IPS device segments. The CoreController can control traffic across its three 10GbE network segment pairs and across multiple TippingPoint E-Series IPS devices. IPS devices are connected by 1GbE uplinks, and each packet that is received on a 10GbE CoreController interface passes through a load balancer that then determines the IPS connection to use for transmitting the packet.
The Core Controller provides:

- 10GbE bidirectional traffic inspection and policy enforcement
- High Availability with an optional Smart ZPHA module
- Central management through the SMS

**Note:** The Core Controller can be used with the 2400E and 5000E IPS devices, and with all N-Series devices.

### High Availability

TippingPoint devices are designed to guarantee that your network traffic always flows at wire speeds in the event of internal device failure. The TippingPoint System provides Network High Availability settings for Intrinsic Network HA (INHA) and Transparent Network HA (TRHA). These options enact manually or automatically, according to settings you enter using the LSM, CLI, or SMS. Zero-Power High Availability (ZPHA) is available for the IPS as an external modular device, and for the Core Controller as an optional Smart ZPHA module.

The IPS uses INHA for individual device deployment and TRHA for devices deployed in redundant configurations in which one device takes over for another in the event of system failure. With INHA, a failure puts the device into Layer-2 Fallback mode and permits or blocks traffic on each segment. In TRHA, multiple IPS devices are synchronized so that when one device experiences a system failure, traffic is routed to the other device with no interruption in intrusion prevention services.

SMS high availability provides continuous administration through an active-passive SMS system configuration. A passive SMS is configured, synchronized with the active system, and waits in standby mode and monitors the health of the active system. If the health or communications check fails, the passive SMS will be activated.

The ZPHA modular device can be attached to an IPS to route traffic in the event of power loss. Smart ZPHA modules perform the same function and are installed directly in the device.

### Threat Suppression Engine

The Threat Suppression Engine (TSE) is a line-speed hardware engine that contains all the functions needed for Intrusion Prevention, including IP defragmentation, TCP flow reassembly, statistical analysis, traffic shaping, flow blocking, flow state tracking and application-layer parsing of over 170 network protocols.

The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. As each new packet of the traffic flow arrives, the engine re-evaluates the traffic for malicious content. The instant the engine detects malicious traffic, it blocks all current and all subsequent packets pertaining to the traffic flow. The blocking of the traffic and packets ensures that the attack never reaches its destination.
The combination of high-speed network processors and custom chips provide the basis for IPS technology. These highly specialized traffic classification engines enable the IPS to filter with extreme accuracy at gigabit speeds and microsecond latencies. Unlike software-based systems whose performance is affected by the number of filters installed, the highly-scalable capacity of the hardware engine allows thousands of filters to run simultaneously with no impact on performance or accuracy.

## Threat Management Center

The Threat Management Center (TMC) is a centralized service center that monitors global threats and distributes up-to-date attack filter packages, software updates, and product documentation.

The Threat Management Center (TMC) collects threat information and creates Digital Vaccine packages that are made available on the TMC web site. The packages include filters that block malicious traffic and attacks on your network. The filters provide the following protections:

- **Application Protection** — Defend against known and unknown exploits that target applications and operating systems:
  - Attack Protection filters — Detect and block traffic known to be malicious, suspicious, and to have known security implications. These filters include the following: Vulnerabilities and Exploits filters.
  - Security Policy filters — Detect and block traffic that may or may not be malicious. This traffic may be different in its format or content from standard business practice, aimed at specific software or operating systems, or contrary to your company's security policies.
  - Reconnaissance filters — Detect and block scans, sweeps, and probes for vulnerabilities and information about your network. These filters include the following: Probes and Sweeps/Scans filters.
  - Informational filters — Detect and block classic Intrusion Detection System (IDS) infiltration

- **Infrastructure Protection** — Protect network bandwidth and network infrastructure elements such as routers and firewalls from attack using a combination of filter types:
  - Advanced DDoS filters — Available on the 2400E and 5000E. Detect and block denial of service and flood requests, such as SYN Requests, that can overwhelm a system.
  - Network Equipment Protection filters — Protect networked equipment from attacks
  - Traffic Normalization filters — Detect and block abnormal or malicious traffic

- **Performance Protection** — Allow key applications to have prioritized bandwidth access setting that ensure mission critical applications have adequate performance during times of high congestion:
  - Misuse and Abuse filters — Protect the resources and usage of file sharing across networks and personal computers. These filters protect peer-to-peer services.
  - Traffic Management filters — Protect the network by shielding against IP addresses or permitting only a set of IP addresses
2

IPS Concepts and the LSM

Overview

The TippingPoint Intrusion Prevention System (IPS) device protects your network by scanning, detecting, and responding to network traffic according to the filters, action sets, and global settings maintained on each device by a client. Each device provides intrusion prevention for your network according to the amount of network connections and hardware capabilities.

The Local Security Manager (LSM) provides a user-friendly, browser-based GUI for administering the IPS.

This chapter describes IPS concepts and the login and navigation procedures of the LSM user interface.

- “IPS Deployment” on page 10
- “Threat Suppression Engine” on page 10
- “IPS Filtering” on page 11
- “Security Notes” on page 15
- “Logging In to the LSM” on page 15
- “The LSM Screen Layout” on page 17
- “System Summary” on page 20
IPS Deployment

A single IPS can be installed at the perimeter of your network, at the network core, on your intranet, or in all three locations. The following diagram shows an example of a corporate network with IPS devices deployed in a variety of locations.

Figure 2 - 1: IPS Deployment Example

Threat Suppression Engine

The main component of the IPS device is the Threat Suppression Engine (TSE), a custom engine that detects and blocks a broad range of attacks at wire speeds. The TSE is a flow-based network security engine, in which each packet is identified as a component of a flow and each flow is tracked in the connection table on the IPS. A flow is uniquely identified by its packet header information:

- IPv4 or IPv6 protocol (ICMP, TCP, UDP, other)
- source and destination IP addresses
- source and destination ports

The TSE reconstructs and inspects flow payloads by parsing the traffic at the application layer. When a packet matches an IPS filter, the IPS handles the packets based on the action set configured on the filter. For example, if the action set is **Block**, then the packet is dropped and subsequent packets from the same flow are dropped without inspection. The IPS device provides default actions to block or permit traffic with options to quarantine or rate-limit traffic and to notify users or systems when an action executes. Logging options are also available to review the types of traffic being filtered by the device. You can customize the default action sets, or create your own based on your network requirements.
IPS Concepts and the LSM

IPS Filtering

The TSE uses Digital Vaccine (DV) filters to police your network and to screen out malicious or unwanted traffic. In addition to the Digital Vaccine filters, the IPS also provides Traffic Management filters, custom filters that react to traffic based on source IP address, destination IP address, port, protocol, or other defined values. Traffic management filters are applied to traffic before Digital Vaccine filters. Depending on how the filters are configured, traffic may or may not require further inspection

The Digital Vaccine Package

DV filters are contained in a Digital Vaccine (DV) package. All IPS devices have a DV package installed and configured to provide out-of-the-box IPS protection for the network. After setting up the IPS, you can customize the filters in the DV through the LSM. To ensure that you have the most up-to-date DV package, use the Update page in the LSM to download the latest package. See “Viewing and Managing Current Digital Vaccine Filters” on page 96.

The filters within the DV package are developed by TippingPoint's Digital Vaccine Labs to protect the network from specific exploits as well as potential attack permutations to address for Zero-Day threats. These filters include traffic anomaly filters and vulnerability-based filters. Vulnerability-based filters are designed to protect the network from an attack that takes advantage of a weakness in application software. For viruses that are not based on a specific vulnerability in software, the DV provides signature filters. TippingPoint delivers weekly Digital Vaccine updates which can be automatically installed on the IPS device (System > Update). If a critical vulnerability or threat is discovered, Digital Vaccine Updates are immediately distributed to customers. See “Enable Auto Update for Digital Vaccine” on page 97.

Tip: In addition to providing a download location for Digital Vaccine packages, the TMC also provides DV product documentation that includes more detailed information about the filters included in the DV package, filter updates, and other related information.

Filter Components

IPS filters have the following components which determine the identity the filter type, global and customized settings, and how the system will respond when the Threat Suppression Engine finds traffic matching the filter:

- **Category**: defines the type of network protection provided by the filter. The category is also used to locate the filter in the LSM and to control the global filter settings using the Category Setting configuration.
- **Action set**: defines the actions that execute when the filter is matched.
- **Adaptive Filter Configuration State**: allows you to override the global Adaptive Filter configuration settings so that the filter is not affected by adaptive filtering. See also “Adaptive Filtering” on page 13
- **State**: Indicates if the filter is enabled, disabled, or invalid. If the filter is disabled, the Threat Suppression Engine does not use the filter to evaluate traffic.
Categories and Category Settings

Categories and category settings are used to configure global settings for all filters within a specified category group. DV Filters are organized into categories and groups based on the type of protection provided:

- **Application Protection Filters** defend against known exploits and exploits that may take advantage of known vulnerabilities targeting applications and operating systems. This filter type includes the sub-categories *Exploits, Identity Theft, Reconnaissance, Security Policy, Spyware, Virus, and Vulnerabilities*.

- **Infrastructure Protection Filters** protect network bandwidth and network infrastructure elements such as routers and firewalls from attack by using protocols and detecting statistical anomalies. These filter types includes the sub-categories *Network Equipment and Traffic Normalization*.

- **Performance Protection Filters** block or rate-limit traffic from applications that can consume excessive bandwidth, leaving network resources available for use by key applications. This filter type includes the sub-categories: *IM, P2P, and Streaming Media*.

Category Settings are used to assign global configuration settings to filters in a sub-category. For example, if you don’t want to use any filters to monitor P2P traffic, you can change the category settings for the Performance Protection, P2P filter group to disable these filters. Category settings consist of the following global parameters:

- **State**: determines whether filters within the sub-category are enabled or disabled. If a category is disabled, all filters in the Category are disabled.

- **Action Set**: determines the action set that filters within a Category will execute when a filter match occurs. If the Recommended action set is configured, filters within the category are configured with the settings recommended by the Digital Vaccine team. If required, you can override the category setting on individual filters by editing the filter to define custom settings.

See “Edit DV Filter Category Settings” on page 34 and “Edit Category Settings for a Filter Group” on page 34.

Filter Override Settings

For the best system performance, TippingPoint recommends that you use global category settings and the Recommended action set for all DV filters. However, in some cases, you may need to override the category settings and recommended action for individual filters due to specific network requirements, or in cases where the recommended settings for a filter interact poorly with your network.

Filter override settings specify custom settings to be applied to the filter in the Security Profile. Once a filter has been customized, it is not affected by the global Category Settings that specify the filter State and Action. See “Edit Individual Filter Settings” on page 36.
Filter Limits and Exceptions

Limits and exceptions change the way filters are applied based on IP address. For example, you can specify a limit setting so that filters only apply to specific source and destination IP addresses or address ranges. If a filter has both global and filter-level exception settings, the Threat Suppression Engine uses the filter-level settings to determine how to apply the filter. You can configure the following limit and exceptions from the LSM:

- **Filter Exceptions** (specific) — Allow traffic that would normally trigger a filter to pass between specific addresses or address ranges without triggering the filter. Configured from the Filter Edit page, these exceptions apply only to the filter where they were configured.

- **Limit Filter to IP Addresses** (global): Only apply filters to traffic between specified source and destination IP address pairs. You can configure IP address limits that apply to all the following filter types: Application Protection, Traffic Normalization, and Network Equipment Protection filters. You can configure separate limits that apply only to Performance Protection filters.

- **Exceptions** (global): Exclude traffic between specified source and destination IP address pairs. You can configure exceptions for the following filter types: Application Protection, Traffic Normalization, Network Equipment Protection, and Performance Protection filters. These exceptions are global for all specified filters.

See “Configure Global IP Address Limits and Exceptions” on page 39.

Adaptive Filtering

With Adaptive Filtering, the Threat Suppression Engine automatically manages filter behavior when the IPS device is under extreme load conditions. This feature protects against the potential adverse affects of a filter that interacts poorly with the network environment by preventing the device from entering High Availability mode. See “Configure Adaptive Filter Settings” on page 61.

Adaptive filtering works by monitoring each filter to identify any suspected of causing congestion. When it identifies a filter, it manages the filter using one of the following methods, depending on how the global or filter-level Adaptive Filtering is configured:

- **Automatic Mode**: This setting enables the IPS device to automatically disable and generate a system message regarding the defective filter.

- **Manual**: This setting enables the IPS device to generate a system message regarding the defective filter. However, the filter is not disabled.
**TippingPoint N Platform Features**

The TippingPoint N Platform enables management of IPv6 traffic and tunneled traffic. The device also permits the use of inspection bypass rules and X.509 certificates.

**Best Effort Mode**

Best Effort mode protects latency-sensitive applications on the network by shunting permitted traffic packets. Best Effort mode is enabled with the following command:

```
debug np best-effort enable [-queue-latency <microseconds>] [-recover-percent <percent>]
```

When Best Effort mode is enabled, the default latency threshold is set at 1000 microseconds, and the default recovery percentage at 20%. The device will enter Best Effort mode when latency reaches 1000 microseconds, and will exit the mode when latency drops to 200 microseconds (20% of 1000).

For detailed information about Best Effort Mode, refer to the *TippingPoint Command Line Interface Reference*.

**IPv6 Inspection and Management**

TOS V 3.1 supports IPv6 traffic inspection, and IPv6 options are available when configuring the Security Profile options. The majority of existing TippingPoint filters are compatible with both IPv4 and IPv6 traffic. The host management port, default gateway, and management port routes can also be configured with IPv6 addresses.

The LSM also includes a Named Networks function, accessible through the System > Named Networks page, which enables you to assign names to specific IPv4 and IPv6 address prefixes.

**Inspection of Tunneled Traffic**

TOS V 3.1 enables inspection of a wide range of tunneled traffic, including:

- GRE (Generic Routing Encapsulation)
- GTP (GPRS Tunneling Protocol)
- Mobile IPv4 (IP-in-IP)
- IPv6, including 6-in-4, 4-in-6, and 6-in-6
- Authentication Header (AH) tunnels
- Tunnels up to 10 layers of tunneling or a header size of 256 bytes.
**Inspection Bypass Rules**

The TippingPoint 2500N and the TippingPoint 5100N enable users to configure inspection bypass rules. Traffic that matches inspection bypass rules is directed through the IPS without inspection. These rules can be applied to traffic according to source or destination IP address, port, or CIDR, or to traffic moving through specific ports.

Inspection bypass rules are defined with the `conf t inspection-bypass` command in the Command Line Interface (CLI). Refer to the *TippingPoint Command Line Interface Reference* for more information.

*Note:* Inspection bypass rules are only enabled on the TippingPoint 2500N and the TippingPoint 5100N.

**Logging In to the LSM**

The IPS device provides simultaneous support for up to 10 web client connections, 10 telnet/SSH (for CLI) connections, and one console connection. Logging in with the CLI is discussed in the *TippingPoint IPS Command Line Interface Reference*.

*Note:* Depending on your security settings, warnings may display when accessing the client. Loading an X.509 certificate will not affect these warnings. See "X.509 Certificates" on page 138.

**Security Notes**

Because the LSM manages the IPS device through a web browser, take the following security precautions.

- Some browser features, such as password caching, are inappropriate for security use and should be turned off.
- The IPS should use the HTTPS server, not the HTTP server. HTTP servers allow usernames and passwords to travel unencrypted over networks and are not secure. You can modify the server configuration using the `conf t server` command. For details, see the Command Line Interface Reference Guide.

*CAUTION:* Failure to follow these security guidelines may compromise the security of your IPS device.
1. In the web browser address bar, enter https:// followed by the IP address or hostname of your IPS device.

The LSM login page appears in the browser. The page displays the name and model of the device.

Figure 2-2: LSM Logon Page

2. Enter your username and password

3. Click Log On. The LSM confirms that your username is valid on the IPS. If the username is valid, the LSM software opens. If the username is not valid, the LSM login page is re-displayed.

After logging in you can access the areas of the LSM permitted by your user role. For information on user roles and access, see Chapter 7, “Authentication”.
The LSM Screen Layout

The LSM screen displays information in the following areas:

- **Menu Bar**: Provides quick access to the System Summary page and the online Help. Displays current user and system status.
- **Navigation**: Provides access to the LSM menu functions.
- **Content and Functionality**: Displays the pages from which you can monitor the device operation and performance, view current configuration settings, and modify configuration. The content refreshes when you click a link in the Navigation pane or when you select buttons or links within a page. When you first log onto the LSM, the System Summary page automatically displays in this area.

![Figure 2 - 3: LSM Screen Layout](image-url)
Menu Bar

The following table lists the available options in the Main Menu Bar:

Table 2 - 1: Main Menu Bar Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Summary</td>
<td>Displays the System Summary. See “System Summary” on page 20.</td>
</tr>
<tr>
<td>Online Help</td>
<td>Launches the online Help.</td>
</tr>
<tr>
<td>Current User</td>
<td>The username of the currently logged-in user.</td>
</tr>
<tr>
<td>Current date and time</td>
<td>The current date and time on the IPS device. The date and time settings on</td>
</tr>
<tr>
<td></td>
<td>the device are determined by the time synchronization method and time</td>
</tr>
<tr>
<td></td>
<td>zone configured for the device. For details, see “Time Options” on page 105.</td>
</tr>
<tr>
<td>Auto Log Off</td>
<td>Logs you out of the LSM. For security purposes, LSM sessions have a</td>
</tr>
<tr>
<td></td>
<td>timeout period. The timeout period sets the length of the idle time before</td>
</tr>
<tr>
<td></td>
<td>the LSM automatically ends the session and logs off the user. The default</td>
</tr>
<tr>
<td></td>
<td>timeout period is 60 minutes. LSM administrators with super-user access</td>
</tr>
<tr>
<td></td>
<td>can change the default timeout period in the Preferences page. See “</td>
</tr>
<tr>
<td></td>
<td>Preferences” on page 136.</td>
</tr>
</tbody>
</table>

Navigation

The following table lists the available options in the navigation area and describes the functionality that each option enables you to access.

Table 2 - 2: Navigation Options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS</td>
<td>• Create and manage security profiles to monitor traffic.</td>
</tr>
<tr>
<td></td>
<td>• Create and manage traffic management filters, action sets, and ports for</td>
</tr>
<tr>
<td></td>
<td>IPS services.</td>
</tr>
<tr>
<td></td>
<td>• Manage and configure settings for IPS filters, the Threat Suppression</td>
</tr>
<tr>
<td></td>
<td>Engine (TSE), and global Adaptive Filters.</td>
</tr>
<tr>
<td></td>
<td>See Chapter 3, “IPS Filtering”.</td>
</tr>
<tr>
<td>Events</td>
<td>• View, download, print, and reset Alert, Audit, Block, and System logs.</td>
</tr>
<tr>
<td></td>
<td>• View graphs reporting on traffic flow, traffic-related events, and</td>
</tr>
<tr>
<td></td>
<td>statistics on triggered filters (attack, rate limit, and adaptive filter).</td>
</tr>
<tr>
<td></td>
<td>• Monitor, search, and maintain traffic streams for adaptive filtering,</td>
</tr>
<tr>
<td></td>
<td>blocked streams, and rate-limited streams.</td>
</tr>
<tr>
<td></td>
<td>• View health information including status of hardware components,</td>
</tr>
<tr>
<td></td>
<td>performance, system health, and system logs.</td>
</tr>
<tr>
<td></td>
<td>• View reports on traffic flow, traffic-related events, and triggered</td>
</tr>
<tr>
<td></td>
<td>filters (attack, rate limit, and adaptive filter).</td>
</tr>
<tr>
<td></td>
<td>See Chapter 4, “Events: Logs, Traffic Streams, Reports”.</td>
</tr>
</tbody>
</table>
Table 2-2: Navigation Options (Continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| System       | • Configure system controls such as the management port, time options, SMS/NMS interaction, High Availability, disk and memory usage thresholds.  
               • Download and install software and Digital Vaccine updates.  
               See Chapter 5, “System”.                                         |
| Network      | • View and configure high availability and link down synchronization settings for segments.  
               • View and configure network ports including options to enable and restart ports.  
               • View and configure virtual ports used to section the network by ports and VLAN IDs.  
               See Chapter 6, “Network”.                                           |
| Authentication| Create, modify, and manage user accounts.                                    
               See Chapter 7, “Authentication”.                                     |

Content and Functionality

The LSM displays all data in the Content and Functionality area. Links selected on these pages may display additional pages or dialog boxes depending on the feature selected.

Title Bar

On each page, you can see the position of the page in the menu hierarchy provided in the title bar. For example, on the Alert Log page, the menu hierarchy indicates that the page is accessed through the Events > Logs sub-menu. You can navigate up the hierarchy from the current location by clicking on the link in the hierarchy listing.

Auto Refresh

Some screens (such as the System Summary screen) automatically refresh themselves periodically. To disable the auto refresh function, deselect the Auto Refresh check box. To manually refresh, click Refresh. To reconfigure the Page Refresh Time, see “Preferences” on page 136.

Tabbed Menu Options

Some sub-menu options are accessible as a tab on the main feature page. For example, on the System > Update page, the following tabs are available: TOS/DV Update, Auto DV Config, and System Snapshots.
System Summary

The System Summary page is the first page that appears when you log onto the LSM. To access the System Summary page at any time, click the View System Summary icon, in the Menu Bar.

The System Summary page includes the following:

- “Health” on page 20
- “Product Specifications” on page 21
- “Reboot Device” on page 21
- “Packet Stats” on page 21
- “Log Summary” on page 22

Health

The Health section of the Statistics frame includes color health indicators for each of the following IPS components:

- System Log
- Performance
- Memory
- Disk
- HA Status
- Power Supply Status
- License

For detailed information about each of the health indicators, click on the corresponding link next to the color indicator. The colors indicate the current state of each component:

- **Green**: No problems
- **Yellow**: Major warning
- **Red**: Critical warning
- **Grey**: Service is disabled

Click Major and Critical warning indicators to view the error that caused the condition. When you view the error, the indicator is reset and its color changes back to green. You can set the warning thresholds on the System > Thresholds page. For more information, see “Set disk usage and memory thresholds” on page 111.
Product Specifications

The Product Specification section displays the following information:

- **Model Number**: Model number of the IPS.
- **Product Code**: The IPS product code.
- **Serial Number**: Serial number of the IPS.
- **TOS Version**: Version number of the TippingPoint Operating System.
- **Digital Vaccine**: Version number of the Digital Vaccine.
- **Reputation**: ReputationDV version. Available only if you have purchased a ReputationDV license.
- **Boot Time**: Time when the IPS was last started.
- **Up Time**: Length of time that the IPS has been operating continuously.

Reboot Device

To reboot the device, click **Reboot**.

Packet Stats

The Packet Stats section provides basic traffic statistics:

- **Received**: Total number of packets received and scanned by the Threat Suppression Engine.
- **Blocked**: Total number of packets that have been blocked by the Threat Suppression Engine.
- **Rate Limited**: The number of packets that matched a filter configured to a permit action set.
- **Trusted**: The number of packets that were passed as trusted.
- **Dropped**: Total number of packets that have been dropped because they are not properly formed or formatted.

To reset the counters, click **Reset**.

Packet counters provide a snapshot of network traffic by displaying the number of packets tracked. If the number is less than 1 million KB, the Packet Stats section displays the full amount. When the number reaches the million and billion mark, the number displays as a decimal amount with a letter (such as G for gigabytes). The unit factors include, M for mega, G for giga, and T for tera. To view the full amount, hover your mouse over the displayed number.

The packet totals give a partial account of blocked activity according to the filters. All other filter results affect the packet totals.

**Note**: The counters are not synchronized with each other. Packets may be counted more than once in some situations.
Log Summary

The Log Summary section displays the number of entries and events for each type of Event Log. In addition, it enables you to download, search, or reset the following logs.

- Alert Log
- Audit Log (Super-User only)
- IPS Block Log
- System Log
- Packet Trace Log

The logs can be reviewed in detail on the Events > Logs page. For more information about logs, see “Logs” on page 64.
Overview

You can monitor and configure the settings for the IPS System from the IPS menu pages.

- **Security Profiles**: View, create, and manage the Security Profiles to provide Digital Vaccine filter coverage across virtual network segments.
- **Traffic Management Profiles**: View, create, and manage the Traffic Management profiles to monitor network traffic based on a limited set of parameters including the source IP address, destination IP address, port, protocol, or other defined values.
- **Action Sets**: View, manage and create actions that define the operations a filter performs when a traffic match occurs.
- **Reputation Groups**: Manage IP Reputation groups, both those made available through the TippingPoint IP Reputation service and those configured manually by the user.
- **Notification Contacts**: Configure notification contacts to send messages to a recipient (either human or machine) in response to a traffic-related event that occurs on the IPS device.
- **IPS Services**: Add and manage non-standard ports supported by the IPS device. Use this feature to configure additional ports associated with specific applications, services, and protocols to expand scanning of traffic. When filters scan traffic against the standard ports for listed services, the engine then accesses and scans traffic against the list of additional ports.
- **Preferences**: Reset IPS filters to the factory default values, configure timeout, logging, and congestion threshold settings to manage performance of the Threat Suppression Engine, configure the Adaptive Filter feature used to protect IPS performance from the effects of over-active filters.
Security Profiles

A Security Profile defines the traffic that the IPS monitors and the DV filters that the IPS applies. Traffic monitoring is based on incoming and outgoing port pairs. You can use the default Digital Vaccine filter configuration to protect the segment or customize the configuration as required. The segment specifies both the port and the traffic direction which allows you to define separate Security Profiles for traffic in and out of a port.

The default security profile is set to ANY incoming ports and ANY outgoing ports, with all IPS filters configured with the default Digital Vaccine settings. With the default profile in place, all incoming and outgoing traffic on any virtual segment configured on the device is monitored according to the IPS filter configuration recommended by TippingPoint. You can edit the default Security Profile to customize the virtual segments that it applies to and modify the filter settings, or create your own Security Profiles as required.

Note: Before creating Security Profiles, verify that the network and system configuration on the IPS device is set up correctly for your environment. In particular, configure all required ports before creating the Security Profiles to protect them.

When a Security Profile is initially created, the recommended settings for all filter categories are enabled.

Use the Security Profiles page to perform the following tasks:

- View, create, edit, and delete Security Profiles
- Change category settings for a group of filters
- Override global filter settings and create filter-level settings
- Restore filter to global category settings
The Security Profile page includes the following information:

**Table 3 - 1: Security Profile Details**

<table>
<thead>
<tr>
<th>Page Section</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Profiles</td>
<td>Profile Name</td>
<td>The name assigned to the Security Profile. The Default Security Profile is pre-configured on the device. You can customize this profile to add virtual segment or modify global and individual filter settings.</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A description of the Security Profile, if a description has been defined.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click to edit the Security Profile.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click to delete the Security Profile.</td>
</tr>
</tbody>
</table>

To manage the virtual segments associated with security profiles, use the Virtual Segments page. See “Virtual Segments” on page 124.

**Note:** If a Traffic Management Profile has been configured with a virtual segment that is not protected by an IPS Security Profile, the segment will be listed in the table in red along with the following message:

No security profile is assigned to the in/out pair. Traffic will **NOT** be inspected by the IPS.

To correct the error, add the segment to an existing Security Profile, or create a new Security Profile to protect it.

See also:

- “Sample Security Profiles” on page 26
- “Applying Security Profiles to Traffic” on page 27
- “Create a Security Profile” on page 28
- “Edit a Security Profile” on page 28
- “IPS Digital Vaccine Filters” on page 29
Sample Security Profiles

The following table shows a sample port configuration for an IPS device:

Table 3 - 2: Port Configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>Network Port</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>ANY</td>
<td>ANY</td>
<td>ANY</td>
</tr>
<tr>
<td>1A</td>
<td>1</td>
<td>ANY</td>
</tr>
<tr>
<td>1B</td>
<td>2</td>
<td>ANY</td>
</tr>
<tr>
<td>Marketing-A</td>
<td>1</td>
<td>6</td>
</tr>
<tr>
<td>Marketing-B</td>
<td>2</td>
<td>6</td>
</tr>
</tbody>
</table>

The following table lists some sample Security Profiles you may create to monitor traffic on a device with the configuration shown above:

Table 3 - 3: Sample Security Profiles

<table>
<thead>
<tr>
<th>Name</th>
<th>Segment(s) (Incoming, Outgoing)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marketing</td>
<td>Marketing-a ==&gt; Marketing-b Marketing-b ==&gt; Marketing-a</td>
<td>Monitor all VLAN 6 traffic on port 1 and port 2 in both directions.</td>
</tr>
<tr>
<td>LAN</td>
<td>1A ==&gt; 1B 1B ==&gt; 1A</td>
<td>Monitor all traffic between port 1 and port 2, except traffic tagged for VLAN 6. VLAN 6 traffic is covered by the Marketing security profile above.</td>
</tr>
<tr>
<td>Default</td>
<td>ANY ==&gt; ANY</td>
<td>Monitor all incoming and outgoing traffic with any port/VLAN ID except traffic on virtual segment 1A ==&gt; 1B. This traffic is already covered by the LAN and Marketing profiles.</td>
</tr>
</tbody>
</table>

Default Security Profile

The default security profile is set to the ANY< ==> ANY virtual segment with all IPS filters configured with the default Digital Vaccine settings. With the default profile in place, all incoming and outgoing traffic in any virtual segment configured on the device is monitored according to the DV filter configuration recommended by TippingPoint.

You can edit the default Security Profile to customize the virtual segments that it applies to and create custom filter settings, or create your own Security Profiles as required. TippingPoint recommends that you keep the default Security Profile with the default virtual segment ANY <==> ANY. This configuration ensures that all traffic will be inspected by the IPS using the default Security Profile, if the traffic does not match a more specific virtual segment configuration.
Applying Security Profiles to Traffic

In the IPS, it is possible for a packet to match more than one Security Profile depending how the virtual segments are configured within each profile. As a general rule, the IPS device will apply the filtering rules specified in the Security Profile that has the most specific virtual segment defined. To determine specificity, the IPS device always considers the incoming zone first. See the following examples to see how the IPS applies filtering rules when a packet matches more than one Security Profile.

Example 1: Packet matches two profiles

Table 3 - 4: Sample Security Profile Zone Configuration

<table>
<thead>
<tr>
<th>Security Profile</th>
<th>Applies To Segment</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>1A (any VLAN) ==&gt; 1B (any VLAN)</td>
</tr>
<tr>
<td>#2</td>
<td>ANY &lt; ==&gt; ANY</td>
</tr>
</tbody>
</table>

With this configuration, a packet going from virtual port 1A to virtual port 1B matches both Security Profile #1 and #2. The IPS device applies the filtering rules from Security Profile #1 to the packet because the virtual port 1A is more specific than the virtual port ANY.

Example 2: Packet matches a profile with specified ports

Table 3 - 5: Sample Security Profile Zone Configuration

<table>
<thead>
<tr>
<th>Security Profile</th>
<th>Applies to Segment(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>ANY &lt;==&gt; ANY</td>
</tr>
<tr>
<td>#2</td>
<td>ANY ==&gt; 1B</td>
</tr>
<tr>
<td>#3</td>
<td>1A ==&gt; 1B</td>
</tr>
</tbody>
</table>

With this configuration, a packet going from the virtual port 1A to 1B matches Security Profiles #1, #2 and #3. However, the IPS device applies filtering rules from Security Profile #3 to the packet because the 1A virtual port is more specific than the virtual port ANY.
Example 3: Packet matches a profile with a specific VLAN tag

Table 3 - 6: Sample Security Profile Zone Configuration

<table>
<thead>
<tr>
<th>Security Profile</th>
<th>Applies to Segment(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>#1</td>
<td>Marketing -a (1A, VLAN 6) ==&gt; Marketing-b (Port 2, VLAN 6) Marketing -b ==&gt; Marketing-a</td>
</tr>
<tr>
<td>#2</td>
<td>1A ==&gt; 1B 1B ==&gt; 1A</td>
</tr>
<tr>
<td>#3</td>
<td>ANY &lt; ===&gt; ANY</td>
</tr>
</tbody>
</table>

With this configuration, a packet tagged as VLAN 6 traveling between 1A and 1B matches all the security profiles. However, the IPS device applies filtering rules from Security Profile #1 because the VLAN 6 tag is the most specific classification criteria.

Create a Security Profile

1. Use the navigation bar to access the Security Profiles page.
3. Enter the Profile Name and, if desired, Description.
4. Apply the security profile to virtual segments in the Virtual Segments section by selecting the virtual segment from the drop-down menu and click Add to table below.
5. If required, modify category settings, filter overrides, limits, and exceptions.
6. Click Create.

Edit a Security Profile

2. Click the name of the profile that you want to edit. The Edit Security Profile page appears.
3. Apply the security profile to virtual segments in the Virtual Segments section by selecting the virtual segment from the drop-down menu and click Add to table below. Click ✗ to delete a virtual segment from the profile.
4. Review or configure additional configuration options. You can modify category settings, filter overrides, DDoS filters, Reputation filters, limits, and exceptions.
5. Click Save to update the Security Profile.

Note: Virtual segments that are associated with only one profile are deleted from the system completely when they are removed from that profile.
IPS Digital Vaccine Filters

IPS Digital Vaccine (DV) Filters monitor traffic passing between network segments. Based on the Security Profiles configured on the device, the IPS applies the filters to traffic on each segment included in the profile. Each Security Profile has its own filter settings. Within a Security Profile, you can accept the recommended settings for a filter category, or, if necessary, customize individual filters based on your network environment and security needs. For detailed information about the concepts behind DV filters, see “IPS Filtering” on page 11.

Categories and category settings are used to configure global settings for all filters within a specified category group. Filter settings are used to override the global settings for individual filters within a category group.

You configure filters separately for each Security Profile configured on the IPS device. When a profile is initially created, all filters are set to the default Category Settings. You can change the Category Settings for filters or edit individual filters from the Edit Security Profile page in the LSM.

Because of the large number of DV filters available on the device, the LSM provides a search interface on the Security Profiles page to view and edit filters. For instructions on using this interface and on editing filters, see the following topics:

- “View DV Filters” on page 30
- “Edit DV Filter Category Settings” on page 34
- “Edit Category Settings for a Filter Group” on page 35
- “Edit Individual Filter Settings” on page 36
- “Configure Global IP Address Limits and Exceptions” on page 39
- “Reset an Individual Filter” on page 40
View DV Filters

You can view and manage the filters configured on a Security Profile with the Filters and Filter Search menu pages. Both pages can be accessed from the Filter Overrides section of the Edit Security Profile pages.

2. Click the name of the profile that you want to edit. The Edit Security Profile page appears.
3. Under Filter Overrides:
   • To access the Filters page, use the View all filters link. See “Filters List” on page 32.
   • To access the Filter Search page, click Search All Filters. See “Filter Search” on page 30.

You can complete the following tasks from these pages:

• View current filters
• Sort the filter list
• Locate a filter or group of filters
• Add a filter to the filter override list for a Security Profile
• Remove a filter from selected Security Profiles
• View the filter description page which includes information about the filter, recommended settings, and the current filter state

Filter Search

The Filter Search page enables you to view all filters or only those matching user-specified search criteria. Access the Filter Search page by clicking Search All Filters while editing a security profile. To sort filter search results, click the appropriate column heading in the Filters List table.

Figure 3 - 1: Filters Page with Search
You can search for filters according to the following parameters:

**Table 3-7: Search Filter Criteria Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keywords</td>
<td>Words or phrases in the filter names. You can search for a specific filter name or for a specific substring in the filter name. A Keyword search is a string search, not a Boolean search, and is not case-sensitive. If you enter a phrase, the results will contain the exact phrase. For example, if you enter “ICMP reply” the search will <strong>not</strong> return a filter whose description is “ICMP: Echo Reply”</td>
</tr>
<tr>
<td>Include Description</td>
<td>Option that expands the search to find the specified keyword(s) in the filter descriptions as well as in the filter names.</td>
</tr>
<tr>
<td>Filter #</td>
<td>The unique filter ID number.</td>
</tr>
<tr>
<td>Filter State</td>
<td>Current operating states. You can select one of the following states: Any, Disabled, or Enabled.</td>
</tr>
<tr>
<td>Filter Control</td>
<td>The filter configuration. You can select one of the following states: Any, Category Settings (defaults), or Override (customized).</td>
</tr>
<tr>
<td>Categories</td>
<td>IPS filter category groups. You can choose from all groups in the Application Protection, Infrastructure Protection, and Performance Protection categories.</td>
</tr>
<tr>
<td>Action Set</td>
<td>Action sets assigned to filters. You can choose from all the default and custom Action Sets configured on the device.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Transport protocols that filters can apply to.</td>
</tr>
<tr>
<td>Severity</td>
<td>Severity Levels assigned to filters.</td>
</tr>
</tbody>
</table>

For details on performing a filter search see the following topics:

- “View Filters with Recommended (Default) Settings” on page 33
- “View Filter Overrides and Custom Settings” on page 34
IPS Filtering

Filters List

The Filters List page lists all filters that are configured on a Security Profile. Access this page by selecting View all filters on the Security Profile page. Because of the large number of filters, it may take some time for the system to display the page.

The Filters List page includes a search form, which includes the same features as the Filter Search page. For more information about the search form, see “Filter Search” on page 30.

The Filters List table includes the following features:

Table 3-8: Filter List Details

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check Box</td>
<td>Selects the filters that you want to add to the security profile. If a filter entry has no check box, that filter has already been added to the Security Profile.</td>
</tr>
<tr>
<td>Filter Name</td>
<td>The unique identifying number and name of the filter. The name includes the protocol to which the filter applies and other descriptive information about the purpose of the filter (0079: ICMP:Echo Reply). These names are assigned by the TippingPoint Digital Vaccine team. Click the name of the filter to view filter information.</td>
</tr>
<tr>
<td>Category</td>
<td>The type of network protection provided by the filter.</td>
</tr>
<tr>
<td>Control</td>
<td>Indicates whether the filter configuration uses the default category settings or user-customized settings. To view and manage customized filters, select the filter from the Filters table on the Security Profile page.</td>
</tr>
<tr>
<td>Action Set</td>
<td>The action set currently assigned to the filter. If the filter uses the default category settings and the action set, the action set will be listed as Disabled. If the filter has an override, the action selected in the override is displayed.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates whether the filter is enabled (in use) or disabled.</td>
</tr>
<tr>
<td>Function(s)</td>
<td>Indicates whether the filter can be added to the security profile.</td>
</tr>
</tbody>
</table>

For details on viewing filters on the Filter List page, see the following topics:

- “View Filters with Recommended (Default) Settings” on page 33
- “View Filter Overrides and Custom Settings” on page 34
Adding a Filter to a Security Profile

There are multiple methods for adding a filter to a security profile:

- Select one or more filters from a filter search. See “View Filters with Recommended (Default) Settings” on page 33.
- Select one or more filters from the Filters List. See “View Filters with Recommended (Default) Settings” on page 33.
- Use the Security Profile section on the View Filter page. See “Edit Individual Filter Settings” on page 36.

View Filters with Recommended (Default) Settings

2. On the Security Profiles page, click on the name of the security profile that you want to edit.
3. In the Filter Overrides section:
   - Select View all filters to view the Filters page. Because of the large number of filters, this action may take some time to execute. You can sort the filters by filter name, control type, action, or state by clicking the appropriate column heading in the Filters List table.
   - Select Search Filters to view the Search Filters page. Enter one or more search parameters and click Search.

In the Filters list generated by View all filters and by filter searches, you can can perform the following tasks:

- View filter details by clicking on the filter name.
- Add a single filter to the current security profile by clicking the green plus-sign icon.
- Add multiple filters to the current security profile by selecting the check boxes next to the filter names and clicking Add Selected Filters.

Select a filter that you want to customize. See “Edit Individual Filter Settings” on page 36.
**View Filter Overrides and Custom Settings**

1. On the LSM menu, click **IPS > Security Profiles**.
2. On the **Security Profiles** page, click on the name of the security profile that you want to edit.
3. In the **Profile Details (Advanced)** table, scroll down to the **Filter Overrides** section.

In the Filter Overrides section, you can can perform the following tasks:

- View and/or edit a filter by clicking on the **Filter Name**.
- Remove the filter override and return the filter to its default settings by clicking the **Delete** icon.

**Edit DV Filter Category Settings**

By default, a Security Profile uses the default category settings for all filters available in the Digital Vaccine package. In some cases you may not need a particular filter or category of filters. For example, if you do not have a particular type of web server installed on your network, you may want to disable filters that protect that type of web server against attack. From the LSM, you can modify the filter configuration for a Security Profile by category or by changing individual filter settings. You can make the following types of changes:

- Edit a Filter Category Group to enable/disable all filters in the group or change the assigned action for all filters in the group.
- Edit an individual filter or group of filters to modify the following settings: State, Action, Adaptive Filter Configuration State, Exceptions.

When you edit a filter, the changes only affect the Security Profile in which you make the edits. This allows you to have different filter configurations for different network segments.

For details on editing filters, see the following topics:

- “Edit Category Settings for a Filter Group” on page 35
- “Edit Individual Filter Settings” on page 36

**Note:** If the category setting is enabled and you disable the filter, the filter may still display as enabled.
Edit Category Settings for a Filter Group

For the best system performance, TippingPoint recommends that you use global Category Settings and the Recommended action set for all DV filters. However, in some cases, you may need to override the category settings and recommended action for individual filters due to specific network requirements, or in cases where the recommended settings for a filter interact poorly with your network. For more information about editing individual filters, see “Edit Individual Filter Settings” on page 36.

Figure 3 - 2: Edit Security Profile Page - Category Settings

When you change the Category Settings for a group of filters, the settings will not affect any filters that have been customized (overridden). Filters that have been customized appear on the Edit Security Profiles page in the Filter Filter Overrides section. On the Filters List page, these filters are listed with Control = Filter.

1. On the LSM menu, click **IPS > Security Profiles**.
2. On the **Security Profiles** page, click on the name of the security profile that you want to edit.
3. On the **Edit Security Profile** page, locate the category in the **Category Settings** table.
4. Modify the settings as required:
   - **State**: Enables or disables all filters in the group.
   - **Action**: Selects the Action Set that will be used for all filters in the group. The Recommended Action Set is the system default for all category groups. If this action is selected, each filter in the group is configured with the settings recommended by TippingPoint. Filters within the group may have different settings for State and Action.
5. Click **Save** (at the bottom of the **Security Profile** page).
Edit Individual Filter Settings

For the best system performance, TippingPoint recommends that you use global Category Settings and the Recommended action set for all DV filters. However, in some cases, your network requirements may require you to override the category settings and recommended action for individual filters. Once a filter has been customized, it is not affected by the global Category Settings that specify the filter State and Action. For more information about editing category settings, see “Edit Category Settings for a Filter Group” on page 35.

1. Search for the filter that you want to modify. See “View Filters with Recommended (Default) Settings” on page 33.

2. On the View Filter page, add the filter to the appropriate security profile by selecting it in the Security Profiles table. After making changes, click Save. The Security Profiles page lists the selected filters in the Filters table.

3. Click the filter name, or the pencil icon. The Edit Filter page appears.

4. Modify the filter settings as required.
   - To use a different action set for the filter, select the Override option in the Action/State section and select the action set that you want to use. To enable or disable the filter, select or deselect the Enabled checkbox.
   - Select the Adaptive Filter Configuration state appropriate to your network.
   - Define IP address exceptions for the filter. Enter source or destination IP addresses and click Add to table below to create IP address exceptions.

5. Click Save.

Note: If the action for the filter is set to Recommended and you do not change it, the filter may remain disabled even when you select the Enabled check box. This happens when the recommended setting for the filter state is Disabled. To enable a filter with this setting, you must change the action from Recommended to another option.

Note: Entering an IPv4-mapped address in IPv6 notation will only match addresses that actually appear in IPv6 packets on the wire. They will not match IPv4 packets. Similarly, a range entered in IPv4 notation will only match IPv4 packets, and not IPv6 packets that contain the equivalent IPv4-mapped addresses. To match both notations, use both.

In fields where “any” is allowed, you may enter “any4” to match IPv4 packets, “any6” to match IPv6 packets, and “any” to match both IPv4 and IPv6 packets.

Note: When using wildcards to create an IPv6 address exception, use a wildcard character to represent each field. For example, input using the following format is valid:

```
a:b:c:d:e:f::*
```

The following format would be rejected as invalid:

```
a:b:c:d:e:* *
```
Create or Edit a DDoS Filter

1. On the LSM menu, click **IPS > Security Profiles.**
2. On the **Security Profiles** page, click on the name of the security profile that you want to edit.
3. On the **Edit Security Profile** page, click **Edit DDoS Filters For This Profile.** The DDoS Filters List page appears.
4. To create a DDoS filter, click **Create DDoS Filter.** To edit an existing filter, click on the filter's name in the list.
5. In the **Filter Parameters** section, do the following:
   - Enter the **Filter Name.**
   - Select the **Action** that determines how the device will manage traffic that triggers the filter: **Block + Notify** or **Block.**
   - Enter a **Destination IP** address or a CIDR to specify a set of IP addresses to which the filter applies.
6. If you have enabled global SYN proxy DDoS protection, specify the threshold for the maximum number of SYN connection requests allowed per second. When the threshold is met, all subsequent SYNs are dropped until the frequency drops below the threshold.
7. Click **Create** or **Save** to return to the DDoS Filters List page.
8. On the DDoS Filters List page, click **Edit Profile** to return to the Security Profile page.

**Note:** DDoS filters will not take effect if asymmetric mode is enabled on the device. See “Configure the Threat Suppression Engine (TSE)” on page 60.
Edit Reputation Filter Settings

2. On the Security Profiles page, click on the name of the security profile that you want to edit.
3. On the Edit Security Profile page, click Edit Reputation Filters For This Profile. The Reputation Filters List page appears.
4. Modify the following settings as needed:
   - Under Apply Reputation Filters, select whether you want the filter to apply to traffic source IP addresses, destination IP addresses, or both. Source and Destination IP Addresses can be entered in CIDR format, as “any”, or as *.
   - Select whether you want packets to be permitted or dropped when reputation lookup is pending.
   - Under Reputation Filter Exception Settings, enter IP addresses or DNS domains to which reputation filters are not applied. The addresses may be source, destination, or both.
5. Click Apply to save the settings and return to the Security Profile page.

   **Note:** For more information about Reputation Groups and ReputationDV, see "Reputation Groups" on page 47.

Create or Edit a Reputation Filter

2. On the Security Profiles page, click on the name of the security profile that you want to edit.
3. On the Edit Security Profile page, click Edit Reputation Filters For This Profile. The Reputation Filters List page appears.
4. Click Create Reputation Filter. The Create Reputation Filter page appears.
5. Select the Reputation Group.
6. Enable the filter by selecting the Enabled check box. Disable the filter by deselecting it.
7. Select the action set that you want to apply to the filter.
8. Enter a traffic threshold.
9. Click Apply to save the filter and return to the Reputation Filters List page.

   **Note:** For more information about Reputation Groups and ReputationDV, see "Reputation Groups" on page 47.
Configure Global IP Address Limits and Exceptions

1. From the LSM menu, click **IPS > Security Profiles**.
2. On the **Security Profiles** page, click on the name of the security profile that you want to edit.
3. In the **Limits/Exceptions** section, add IP addresses to Application Protection Filter Exclusives, Application Protection Filter Exceptions, and Performance Protection Filter Exclusives:
   
   **A.** Enter the **Source Address**. Source and Destination IP Addresses can be entered in CIDR format, as “any”, or as *.  
   **B.** Enter the **Destination Address**.  
   **C.** Click **Add to table below**.  
   **D.** Repeat this process for each IP address exception required.  

4. Click **Apply**.

**Note:** Entering an IPv4-mapped address in IPv6 notation will only match addresses that actually appear in IPv6 packets on the wire. They will not match IPv4 packets. Similarly, a range entered in IPv4 notation will only match IPv4 packets, and not IPv6 packets that contain the equivalent IPv4-mapped addresses. To match both notations, use both.

In fields where “any” is allowed, you may enter “any4” to match IPv4 packets, “any6” to match IPv6 packets, and “any” to match both IPv4 and IPv6 packets.

**Note:** When using wildcards to create an IPv6 address exception, use a wildcard character to represent each field. For example, input using the following format is valid:

```
a:b:c:d:e:f:::*:*  
```

The following format would be rejected as invalid:

```
a:b:c:d:e:*  
```

Delete a Global Limit/Exception Setting

1. From the LSM menu, click **IPS > Security Profiles**.
2. On the **Security Profiles** page, click on the name of the security profile that you want to edit.
3. In the **Limits/Exceptions** section, review the global limit and exception address entries. Click ✗ to delete an entry.

4. Click **Apply**.

To delete a filter-level exception, edit the filter. For details, see “Edit Individual Filter Settings” on page 36.
Reset an Individual Filter

If you have created a filter override in a Security Profile, you can restore the filter to its default settings by deleting the filter from the Security Profile Filters table.

1. From the LSM menu, click **IPS > Security Profiles**.
2. On the **Security Profiles** page, click on the name of the security profile that you want to edit.
3. In the **Filter Overrides** table, find the entry for the filter override you want to remove and click ✗. The filter is restored to the recommended settings for the category it belongs to.

You can also reset all filters to their factory default settings from the IPS Preferences page. For details, see “Reset Security Policy” on page 59.

**CAUTION:** If you use the IPS Preferences page to reset the filters to their default settings, all filters will be set to their recommended state and all user-customized action sets, rate limits, and thresholds will be deleted. You will also lose the Security Profiles and custom Security Profile settings that you have created.
Traffic Management Profiles

Use the Traffic Management Profiles page (IPS > Traffic Management Profiles) to view, create, edit, or delete a Traffic Management profile and apply Traffic Management profiles to virtual segments. A Traffic Management Profile consists of the following components:

- **Identification**: Profile name and description
- **Virtual Segments**: Specifies the incoming and outgoing virtual ports to which the Traffic Profile applies.
- **Traffic Management Filters**: one or more filters to manage the traffic based on Protocol or IP address and port. Each filter defines the type of traffic to be monitored and the action to be taken when the filter is triggered: Block, Allow, Rate Limit, or Trust.

Traffic that triggers the traffic management filter is managed based on the filter action configured which can be any of the following:

- **Block**: traffic that triggers the filter is denied.
- **Allow**: allows traffic that meets the filter criteria.
- **Rate Limit**: rate limits traffic that meets the filter criteria.
- **Trust**: allows traffic that meets the filter criteria through the IPS device without being inspected.

Traffic that is allowed or rate-limited based on a traffic management filter goes on to be inspected based on the Security Profile configuration (DV filtering). In other words, traffic is not allowed through the device based solely on the traffic management filter criteria, unless the filter is configured with the Trust action.

The Traffic Management Profiles page includes the following information:

**Table 3 - 9: Traffic Management Profile Details**

<table>
<thead>
<tr>
<th>Page Section</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Profiles</td>
<td>Profile Name</td>
<td>The name assigned to the Traffic Management Profile.</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A description of the Traffic Management Profile, if a description has been defined.</td>
</tr>
<tr>
<td></td>
<td>Pencil</td>
<td>Click to edit the Traffic Management Profile.</td>
</tr>
<tr>
<td></td>
<td>Trash Can</td>
<td>Click to delete the Traffic Management Profile.</td>
</tr>
</tbody>
</table>
To manage the virtual segments associated with security profiles, use the Virtual Segments page. See “Virtual Segments” on page 124.

**Note:** The segment that you select must be configured on an IPS Security Profile. Otherwise, traffic on the segment is not inspected by the IPS Digital Vaccine filters. If a Traffic Management filter has been configured with a segment that is not protected by an IPS Security Profile, the segment will be listed in the Security Profile Virtual Segments table in red along with the following message.

No security profile is assigned to the in/out pair. Traffic will NOT be inspected by the IPS.

To correct the error, add the segment to an existing Security Profile, or create a new Security Profile to protect it.

This section discusses the following topics:

- “Applying Traffic Management Profiles to Traffic” on page 42
- “Create a Traffic Management Profile” on page 43
- “Edit a Traffic Management Profile” on page 44
- “Traffic Management Filter Parameters” on page 45
- “Configure a Traffic Management Filter” on page 46

### Applying Traffic Management Profiles to Traffic

You can use traffic management filters to prioritize traffic or implement security policy. For example, you might define the following IP filters for your Web servers in a lab that denies access to external users:

- Block traffic if the source is on an external subnet that arrives through port 80 and is destined for the IP address of your Web server.
- Block traffic if the source is your Web server, the source port is 80, and the destination is any external subnet.

You can define multiple traffic management rules in each profile. In general, when defining filters for network segments more specific filters should come first. For example, a more specific IP filter might block traffic with fully qualified source and destination IP addresses and ports. More general ones, like those that apply to subnets, should follow.
The following table lists several examples of traffic management filters:

Table 3 - 10: IP Filter Settings

<table>
<thead>
<tr>
<th>Source Address</th>
<th>Destination Address</th>
<th>Protocol</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>any</td>
<td>UDP</td>
<td>any</td>
<td>53</td>
<td>Allow</td>
</tr>
<tr>
<td>any</td>
<td>any</td>
<td>UDP</td>
<td>any</td>
<td>any</td>
<td>Block</td>
</tr>
<tr>
<td>any</td>
<td>any</td>
<td>ICMP</td>
<td>any</td>
<td>any</td>
<td>20 Mbps rate-limit</td>
</tr>
<tr>
<td>any</td>
<td>1.2.3.4</td>
<td>TCP</td>
<td>any</td>
<td>80</td>
<td>Allow</td>
</tr>
<tr>
<td>any</td>
<td>any</td>
<td>TCP</td>
<td>any</td>
<td>80</td>
<td>Block</td>
</tr>
<tr>
<td>66.94.234.13</td>
<td>any</td>
<td>IP</td>
<td>any</td>
<td>80</td>
<td>Block</td>
</tr>
</tbody>
</table>

These filters perform the following actions:

- Block all UDP traffic except DNS requests. DNS requests are inspected for attacks.
- Limit all ICMP traffic to 20 Mbps
- Block all HTTP traffic except for server 1.2.3.4
- Block IP fragments coming from IP address 66.94.234.13 on any port going to port 80.

Create a Traffic Management Profile

1. From the LSM menu, click IPS > Traffic Management Profiles.
2. Click Create Traffic Mgmt Profile.
3. On the Create Traffic Management Profiles page, enter the Profile Name. You may also enter a description of the profile.
4. Apply the security profile to virtual segments in the Virtual Segments section by selecting the virtual segment from the drop-down menu and click Add to table below.
5. Repeat this process until you have added all the required virtual segments.
6. Click Create.

After creating the Traffic Management profile, you need to edit it to add traffic management filters. See “Edit a Traffic Management Profile” on page 44.

Note: The virtual segment that you specify must also be assigned to a Security Profile. For details, see the virtual segments field description in Table 3 - 9, “Traffic Management Profile Details,” on page 41.
Edit a Traffic Management Profile

1. On the LSM menu, click **IPS > Traffic Management Profiles**.

2. On the **Traffic Management Profiles** page, click on the name of the traffic management profile that you want to edit.

3. Apply the security profile to virtual segments in the **Virtual Segments** section by selecting the virtual segment from the drop-down menu and click **Add to table below**. Click ✗ to delete a virtual segment from the profile.

4. Review additional configuration options. Perform the following tasks as needed:
   - To add a traffic management filter, click **Add Traffic Management filter**. For details on creating a traffic management filter, see “Configure a Traffic Management Filter” on page 46.
   - To change the precedence of traffic management filters, drag and drop the filter to the appropriate position in the filter list.
   - To edit an existing traffic management filter, click either the filter name or ✉️ in the Functions column.
   - To delete an existing filter, click ✗.

After you have completed the changes, click **Save** to update the Traffic Management Profile.

**Note:** Virtual segments that are associated with only one profile are deleted from the system completely when they are removed from that profile.
Traffic Management Filter Parameters

The following table describes the configuration parameters for traffic management filters.

Table 3 - 11: Traffic Management Filter

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name assigned to the traffic management filter.</td>
</tr>
<tr>
<td>State: Enabled</td>
<td>Indicates the current filter status. A check mark indicates the filter is enabled. You can disable the filter by removing the check mark. You cannot view or change the filter state until you create and save the traffic management filter. The filter is enabled by default.</td>
</tr>
<tr>
<td>Action</td>
<td>Indicates how the IPS device will manage traffic that triggers the filter. The following options are available:</td>
</tr>
<tr>
<td></td>
<td>Block: traffic that triggers the filter is denied.</td>
</tr>
<tr>
<td></td>
<td>Allow: allows traffic that meets the filter criteria.</td>
</tr>
<tr>
<td></td>
<td>Rate Limit: rate limits traffic that meets the filter criteria.</td>
</tr>
<tr>
<td></td>
<td>Trust: for trusted servers or traffic, allows traffic that meets the filter criteria to pass through the IPS device without being inspected.</td>
</tr>
<tr>
<td>Protocol</td>
<td>Specifies the protocol the filter checks for: IP, ICMP, TCP, or UDP.</td>
</tr>
<tr>
<td></td>
<td>• To apply the filter only to IP fragments, select Apply only to IP fragments.</td>
</tr>
<tr>
<td></td>
<td>• To change the protocol to IPv6 and IPv6 equivalents, select IPv6. Selecting ICMP and IPv6 changes the protocol to ICMPv6.</td>
</tr>
<tr>
<td>Source Address and Port</td>
<td>Specifies the source IP address for traffic that will be managed by the filter.</td>
</tr>
<tr>
<td>Destination IP Address and Port</td>
<td>Specifies the destination IP address for traffic that will be managed by the filter.</td>
</tr>
<tr>
<td>ICMP</td>
<td>If the filter applies to ICMP traffic and you want to monitor a specific type of ICMP message, this parameter specifies the ICMP message Type and Code.</td>
</tr>
</tbody>
</table>
Configure a Traffic Management Filter

Traffic management filters are configured in the context of a Traffic Management Profile that determines which network segments are monitored by the filter. For details on creating a profile, see “Create a Traffic Management Profile” on page 43.

2. On the Traffic Management Profiles page, click on the name of the traffic management profile that you want to edit.
3. In the Profile Details (Advanced) section in the Filters table, click Add Traffic Management filter. To edit an existing filter, click the filter name.
4. Enter or edit the filter Name.
5. Select the parameters for the filter:
   - Use the State field to enable or disable the filter. When you create a new filter, it is enabled by default.
   - Select either Block, Allow, Rate Limit and a rate limit action set, or Trust for the Action. Trusted traffic will not be inspected by the IPS.
   - Select the Protocol this filter checks for from the drop-down list: IP, ICMP, TCP, or UDP.
   - To change the protocol to IPv6 and its equivalents, select IPv6. If this option is selected, only IPv6 addresses are allowed. If unselected, only IPv4 addresses are allowed.
   - For the Source and Destination, type the IP Address and Port (if applicable) that identifies the traffic to be monitored. IP addresses can be specified in CIDR format, as “any” or as *. Click IPv6 Info for more information about using IPv6 addresses.
   - If the protocol type is ICMP and you only want to monitor specific ICMP traffic, enter the ICMP Type and Code (0-255).
6. Click Create or Save to return to the Edit Traffic Management Profile page.
7. Click the Save button to update the profile with the new filter information.

**Note:** Entering an IPv4-mapped address in IPv6 notation will only match addresses that actually appear in IPv6 packets on the wire. They will not match IPv4 packets. Similarly, a range entered in IPv4 notation will only match IPv4 packets, and not IPv6 packets that contain the equivalent IPv4-mapped addresses. To match both notations, use both.

In fields where “any” is allowed, you may enter “any4” to match IPv4 packets, “any6” to match IPv6 packets, and “any” to match IPv4 or IPv6 packets depending on whether IPv6 is selected.

**Note:** When using wildcards to create an IPv6 address exception, use a wildcard character to represent each field. For example, input using the following format is valid:

```
a:b:c:d:e::f:*:*:
```

The following format would be rejected as invalid:

```
a:b:c:d:e:
```
Reputation Groups

As a part of security profiles, users can create groups of IP addresses and DNS names, known as reputation groups. Reputation filters enable you to apply block, permit, or notify actions across an entire reputation group.

When an IP address or DNS name is added to a reputation group, it is added to the device's reputation database. Incoming traffic is checked against the database, and the appropriate reputation filters are then applied. While the address or name is being looked up, you may choose to have packets from a suspect address dropped or permitted. See “Create or Edit a Reputation Filter” on page 38 for more information.

The TippingPoint SMS offers additional reputation features; refer to the Tipping Point Security Management System User Guide for more information.

Use the Reputation Groups page to perform the following tasks:

- View existing reputation groups
- Manually create reputation groups
- Access Security Profile pages to create and edit reputation group filters

The Reputation Group feature enables you to create groups of IPv4, IPv6, and DNS addresses and define an action set to apply to all of those addresses.

The Reputation Groups page lists the following information:

**Table 3 - 12: Security Profile Details**

<table>
<thead>
<tr>
<th>Page Section</th>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reputation Groups List</td>
<td>Profile Name</td>
<td>The name assigned to the Reputation Group.</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A description of the Reputation Group, if a description has been defined.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click to edit the Reputation Group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click to delete the Reputation Group.</td>
</tr>
<tr>
<td>Security Profiles</td>
<td>Profile Name</td>
<td>The name assigned to the Security Profile that has reputation filters configured on it.</td>
</tr>
<tr>
<td></td>
<td>Description</td>
<td>A description of the Security Profile, if a description has been defined.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click to edit the Security Profile.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click to delete the Security Profile.</td>
</tr>
</tbody>
</table>
This section discusses the following topics:

- “Create a Reputation Group” on page 48
- “Create a Reputation Filter” on page 48
- “Edit a Reputation Filter” on page 49

Create a Reputation Group

1. Click Create Reputation Group to access the Create Reputation Groups page.
2. Enter a name for the reputation group.
3. Enter a brief description of the group.
4. Enter an IPv4, IPv6, or DNS address in the Address field.
5. Click Add to table below to add the address to the group.
6. Repeat steps 4-5 until you have added all of the addresses that you want to add to the group.
7. Click Create.

Create a Reputation Filter

1. On the Reputation Groups page, click the pencil icon next to the name of the Security Profile to which you want to add a reputation filter. The Reputation Filters List page appears.
2. Click Create Reputation Filter. The Create Reputation Filter page appears.
3. In the Filter Parameters section, do the following:
   - Enter the Filter Name.
   - Select the Action that determines how the device will manage traffic that triggers the filter: Block + Notify or Block.
   - Enter a Destination IP address or a CIDR to which the filter applies.
4. If you have enabled global SYN proxy DDoS protection, specify the threshold for the maximum number of SYN connection requests allowed per second. When the threshold is met, all subsequent SYNs are dropped until the frequency drops below the threshold.
5. Click Save to return to the Reputation Filters List page.
**Edit a Reputation Filter**

1. On the Reputation Groups page, click the **pencil** icon next to the name of the Security Profile to which you want to add a reputation filter. The Reputation Filters List page appears.

2. Click the **pencil** icon next to the name of the Reputation Filter that you want to edit. The Create Reputation Filter page appears.

3. In the **Filter Parameters** section, do the following:
   - Enter the **Filter Name**.
   - Select the **Action** that determines how the device will manage traffic that triggers the filter: **Block + Notify** or **Block**.
   - Enter a **Destination IP** address or a CIDR to specify a set of IP addresses to which the filter applies.

4. If you have enabled global SYN proxy DDoS protection, specify the threshold for the maximum number of SYN connection requests allowed per second. When the threshold is met, all subsequent SYNs are dropped until the frequency drops below the threshold.

5. When editing a Reputation filter, you can also add exceptions.

6. Click **Save** to return to the Reputation Filters List page.

**Delete a Reputation Filter**

1. On the DDoS page, click the **pencil** icon next to the name of the Security Profile from which you want to delete a reputation filter. The Reputation Filters List page appears.

2. Click the **Delete** icon next to the name of the DDoS filter that you want to delete.

3. Confirm that you want to delete the filter.
IPS Filtering

Action Sets

Action Sets determine what the IPS device does when a packet triggers a filter. An action set can contain more than one action, and can contain more than one type of action. The types of action that can be specified include the following:

- **Actions** determine where a packet is sent after it is inspected:
  - A *permit* action allows a packet to reach its intended destination.
  - A *block* action discards a packet. A block action can also be configured to *quarantine* the host and/or perform a *TCP reset*.
  - A *rate limit* action enables you to define the maximum bandwidth available for the traffic stream.
  - A *trust* action allows the designated traffic to bypass all inspection; the traffic is transmitted immediately. *Trust* has lower latency than *Permit*, and using it can reduce load on the CPU and processors.

- **Packet Trace** allows you to capture all or part of a suspicious packet for analysis. You can set the packet trace priority and packet trace verbosity for action sets.

- **Priority** sets the relative importance of the information captured. Low priority items will be discarded before medium priority items if there is a resource shortage.

- **Verbosity** determines how much of a suspicious packet will be logged for analysis. If you choose *full* verbosity, the whole packet will be recorded. If you choose *partial* verbosity, you can choose how many bytes of the packet (from 64 to 1600 bytes) the packet trace log records.

- **Notification Contacts** indicate the contacts to notify about the event. These contacts can be systems, individuals, or groups.

  **Note:** You must create or modify a notification contact before configuring an Action Set that uses the contact. For details, see “*Notification Contacts*” on page 54.

You can also configure a Block action to perform a TCP Reset. This option resets the TCP connection for the source or destination IP when the Block action executes.

  **Note:** Globally enabling the TCP Reset option may negatively impact your system performance. TippingPoint recommends using this option for issues related to mail clients and servers on email related filters.

Use the Action Sets page to perform the following tasks:

- View and manage existing actions
- Create and Edit action sets

Action sets determine what the IPS device does when a packet triggers a filter. An action set can contain more than one action, and can contain more than one type of action.
The Action Sets page lists the following actions:

### Table 3 - 13: Action Sets

<table>
<thead>
<tr>
<th>Action Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recommended</td>
<td>The default Action Set as determined by the filter’s Category Settings. When this action set is assigned to a filter, the filter uses the recommended action setting for the default Category Settings. The Recommended action set may enable different configurations for filters within the same category. Under a Recommended category setting, some filters may be disabled while others are enabled; some may have permit actions assigned while others are set to block.</td>
</tr>
<tr>
<td>Block (+TCP Reset)</td>
<td>Blocks a packet from being transferred to the network. TCP Reset is an option for resetting blocked TCP flows.</td>
</tr>
</tbody>
</table>
| Block + Notify (+TCP Reset) | • Blocks a packet from being transferred.  
• Notifies all selected contacts of the blocked packet.  
TCP Reset is an option for resetting blocked TCP flows. |
| Block + Notify + Trace (+TCP Reset) | • Blocks a packet from being transferred.  
• Notifies all selected contacts of the blocked packet.  
• Logs all information about the packet according to the packet trace settings.  
TCP Reset is an option for resetting blocked TCP flows. |
| Permit + Notify | Permits a packet and notifies all selected contacts of the packet. |
| Permit + Notify + Trace | • Permits a packet.  
• Notifies all selected contacts of the packet, and logs all information about the packet according to the packet trace settings. |
| Trust | • Not configured on the device by default; you must create a Trust action set for this action to appear on the table.  
• Allows trusted traffic to pass without inspection.  
• Lower latency than Permit.  
• Cannot be used with DDoS or IP Reputation filters. |

The Action Sets page provides the following information for each Action configured on the device:

### Table 3 - 14: Action Sets Details

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action Set</td>
<td>The name of the action set</td>
</tr>
<tr>
<td>Action(s)</td>
<td>The actions included in the action set</td>
</tr>
<tr>
<td>TCP Reset</td>
<td>Indicates whether the option to reset a TCP connection is enabled. With TCP reset enabled, the system resets the TCP connection for the source or destination IP when the Block action executes. This option can be configured on Block action sets.</td>
</tr>
<tr>
<td>Packet Trace</td>
<td>Indicates whether packet tracing is enabled</td>
</tr>
</tbody>
</table>
This section discusses the following topics:

- “Special Types of Action Sets” on page 52
- “Configure an Action Set” on page 53

## Special Types of Action Sets

By default, Block and Permit action sets are configured on the IPS. You can also create Rate Limit and Quarantine action sets.

### Rate Limit Action Set

A Rate Limit action set defines a maximum bandwidth that can be used by traffic that matches filters assigned to that action set. Incoming traffic in excess of this bandwidth is dropped. If two or more filters use the same rate limiting action set, then all packets matching these filters share the bandwidth. For example, if filters 164 (ICMP Echo Request) and 161 (ICMP Redirect Undefined Code) use the same 10 Mbps action set, then both “Echo Requests” and “Redirect Undefined Codes” filters share the 10 Mbps “pipe” as opposed to each filter getting a dedicated 10Mbps pipe.

The supported rates are subject to restrictions based on the device model. Any of these listed rates can be used as long as it does not exceed 25% percent of the total bandwidth of the product.

### Quarantine actions

Quarantine allows the system to block packets based on the IP addresses in the packet that triggers the filter. When a filter with a quarantine option is triggered, the system installs two blocks: one for the flow (as is normally done with Block actions) and another for the quarantined IP address. In addition to installing the two blocks, the system quarantines the IP address based on the instructions in the action set.

Quarantine actions can also occur at a user-defined threshold. You can configure permit and trust actions to take effect before the threshold is triggered.

For example, you can display a Quarantine web page to notify a quarantined user of the problem and provide instructions for fixing it, or the action may redirect all traffic from the quarantined IP address to a quarantine server that provides instructions to correct the problem.
Configure an Action Set

1. On the LSM menu, click IPS > Action Sets.
2. On the Action Sets page, click Create Action Set. To edit an existing action set, click the action set name.
3. Enter or edit the action set name.
4. Select the parameters for the action set:
   - 
   - Permit: Allows traffic.
   - Rate Limit: Limits the speed of traffic. You must select a Rate.
   - Block: Blocks traffic from entering the network.
   - TCP Reset: Used with the Block action, resets the source, destination, or both IPs of an attack. This option resets blocked TCP flows.
   - Trust: Allows traffic to pass without inspection.
   - Packet Trace: Enables or disables packet tracing. Specify Priority and Verbosity; if you choose partial verbosity, enter the number of bytes to capture (between 64-1600).
5. Select the contact that will be notified when the action occurs. If there are no contacts displayed, you must create an Email or SNMP Notification Contact first. See “Create an Email or SNMP Notification Contact” on page 57.
6. If desired, select the quarantine options for the action set:
   - No: The action set does not include a Quarantine action.
   - Immediate: When the action set is triggered, the quarantine goes into immediate effect.
   - Quarantine After: When the desired threshold is reached, the quarantine goes into effect.
   - HTTP Traffic options: HTTP requests from the quarantined host can be blocked, redirected to a web server, or redirected to a custom page that displays information about the filter that triggered the quarantine action.
   - Non-HTTP Traffic: Non-HTTP requests can be blocked or permitted.
   - Limit quarantine to the following IP address(es): Enables the quarantine to be restricted to a limited set of hosts.
   - Do not quarantine the following IP address(es): Enables a whitelist of hosts that will not be quarantined.
   - Allow quarantined hosts to access the following IP address(es): Enables quarantined hosts to access selected IP addresses.
7. Click Create or Save.
Notification Contacts

Configure notification contacts to send messages to a recipient (either human or machine) in response to a traffic-related event that occurs on the IPS device. The traffic-related event can be the result of triggering an IPS filter configured with an action set that specifies a notification contact. A notification contact can be any of the following:

- **Remote System Log**: Sends messages to a syslog server on your network. This is a default contact available in all IPS action sets. Before using this contact, configure the IP address and port for the syslog server (System > Syslog Servers).
- **Management Console**: Sends messages to the LSM or the SMS device management application. This default contact is available in all action sets. If this contact is selected messages are sent to the Alert or IPS Block Log in the LSM, depending on whether a permit or block action has executed. When the device is under SMS management, messages are also sent to the SMS client application. This notification contact does not require any configuration, although you can change the default name and aggregation period.
- **Email or SNMP**: Sends messages to the email address or specified SNMP. All email or SNMP contacts must be added from the Notification Contacts page. If the default email server is not configured on the device, you will be prompted to configure it before adding a contact.

**Note**: Before creating an Email or notification contact, you must configure Email and SMTP server settings on the IPS device from the Email Server page. For details, see "Email Server" on page 111.

After configuring notification contacts, you can select them for IPS filter events when you create or edit the action set assigned to the filter.

Use the Notification Contacts page to perform the following tasks:

- View existing notification contacts
- Add new contacts

The Notification Contacts page lists the following information:

**Table 3 - 15: Contacts List**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact Name</td>
<td>The name assigned to the contact.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of contact. The type may be MGMT, SYSLOG, or Email.</td>
</tr>
<tr>
<td>Period</td>
<td>The aggregation period, in minutes, for the contact.</td>
</tr>
<tr>
<td>Other Parameters</td>
<td>Other information about the contact. For example, the Remote System Log contact will show the number of remote syslog servers configured for the device.</td>
</tr>
<tr>
<td>Function(s)</td>
<td>Click on these icons to edit or delete a contact.</td>
</tr>
</tbody>
</table>

**Note**: The Management Console and Remote System Log cannot be deleted from this list.
This section discusses the following topics:

- “Alert Aggregation and the Aggregation Period” on page 55
- “Configure the Management Console Contact” on page 55
- “Configure the Remote System Log Contact” on page 56
- “Create an Email or SNMP Notification Contact” on page 57
- “Delete a Notification Contact” on page 57

Alert Aggregation and the Aggregation Period

The IPS uses Alert Aggregation to prevent system performance problems resulting from an excessive number of notification requests. Because a single packet can trigger an alert, attacks with large numbers of packets could potentially flood the alert mechanism used to send out notifications. Alert aggregation allows you to receive alert notifications at intervals to prevent this flooding. For example, if the aggregation interval is 5 minutes, the system sends an alert at the first IPS filter trigger, collects subsequent alerts and sends them out every five minutes.

On the IPS, alert aggregation is controlled by the aggregation period that you configure when you create a notification contact. This setting is required for all notification contacts.

**CAUTION:** Short aggregation periods can significantly affect system performance. The shorter the aggregation period, the higher the system load. In the event of a flood attack, a short aggregation period can lead to system performance problems.

In addition to the user-configured aggregation period, the system also provides alert aggregation services to protect the system from over-active filters that can lower performance.

For email contacts, the aggregation period works in conjunction with the email threshold setting configured for the email server. See "Email Server” on page 111.

Configure the Management Console Contact

1. On the LSM menu, click **IPS > Notification Contacts**.
2. On the Notification Contacts page, click **Management Console**.
3. Edit the **Contact Name**. By default, it is **Management Console**.
4. Enter the **Aggregation Period** for notification messages in minutes.
5. Click **Save**.
Configure the Remote System Log Contact

Designating a remote system log as the notification contact sends messages to a syslog server on your network. This is a default contact available in all IPS action sets. Before using this contact, configure the IP address and port for the syslog server (System > Syslog Servers).

**CAUTION:** Remote syslog, in adherence to RFC 3164, sends clear text log messages using the UDP protocol with no additional security protections. You should only use remote syslog on a secure, trusted network to prevent syslog messages from being intercepted, altered, or spoofed by a third party.

1. On the LSM menu, click **IPS > Notification Contacts**.
2. On the Notification Contacts page, click **Remote System Log**.
3. Enter the remote system log’s host IP address and port number.
4. Select an **Alert Facility** and a **Block Facility**: none or select from a range of 0 to 31. The syslog server uses these numbers to identify the message source.
5. Select a **Delimiter** for the generated logs: **tab**, **comma**, **semicolon**, or **bar**.
6. Enter a **Remote system log aggregation period** in minutes.
7. Click **Add to table below** to add the remote syslog server.
8. Repeat steps 3-7 to add additional remote system log servers.
9. Click **Save** to save the changes.

Tip: Verify that your IPS can reach the remote system log server on your network. If the remote system log server is on a different subnet than the IPS management port you may need to configure the routing. For details, see “**Management Routing**” on page 103.
Create an Email or SNMP Notification Contact

1. On the LSM menu, click IPS > Notification Contacts.
2. Click Add Contact.
3. On the Create Contact page, select Email or SNMP.
4. Enter the contact name.
5. Enter the Aggregation Period. Longer aggregation periods improve system performance.
6. If the contact is an email contact, enter the address where notifications will be sent in the To Email Address field. If the contact is an SNMP contact, enter the host IP address and port number.
7. Click Create to save the changes.

Note: SNMP notification contacts require SNMPv2, and will not work when SNMPv2 is disabled. See “Configure SMS Information” on page 107 and “View or Configure NMS Information” on page 107.

Note: Before creating an Email or notification contact, you must configure Email and SMTP server settings on the IPS device from the Email Server page. For details, see “Email Server” on page 111.

If the email is not sent correctly, ensure that:

- the default email server is configured. See “Email Server” on page 111.
- the email server is reachable from the IPS.
- the email allows mail relaying and that you use the account/domain that the email server accepts.

Delete a Notification Contact

You cannot delete the default Remote System Log and Management Console contacts or a Notification Contact if it is currently configured on another Action Set.

1. On the LSM menu, click IPS > Notification Contacts.
2. On the Notification Contacts page, click the Delete button.
3. On the confirmation dialog, click OK.
Services

Use the IPS Services page to configure additional ports associated with specific applications, services, and protocols to expand the range of traffic scanned by the IPS device. During the inspection process, the IPS device first scans traffic against the standard ports for listed services, and then scans traffic against the list of additional ports. You can configure up to 16 additional ports for each service.

The IPS Services page provides the following information:

Table 3-16: IPS: IPS Services Details

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Type of application or network service.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The protocol for the application.</td>
</tr>
<tr>
<td>User-Defined Ports</td>
<td>The list of the custom ports defined on the IPS.</td>
</tr>
<tr>
<td>System-Defined Ports</td>
<td>The list of supported ports per application.</td>
</tr>
</tbody>
</table>

This section discusses the following topics:

- “Add a Port” on page 58
- “Delete a Port” on page 59

Add a Port

1. From the LSM menu, click IPS > Services.
2. On the IPS Services page, click Add Port Configuration.
3. On the Create Port Configuration page in the Application Type/Port Assignment section, select the Application Type and enter a Port Number.
4. Click Create and click OK on the confirmation pop-up.

⚠️ CAUTION: TippingPoint does not recommend configuration of user-defined, non-standard ports. Enabling non-standard ports may have a detrimental effect on the performance of the device.
Delete a Port
You can only delete custom ports configurations. You cannot delete any of the default port configurations configured on the IPS device. You can only delete one port at a time.

1. From the LSM menu, click IPS > Services.
2. On the IPS Services page, click Delete Port.
3. On the Delete Port Configuration page, select the Application Type for the port configuration to delete. The selection list only includes applications that have been configured with a custom port.
4. Select the Port Number that you want to delete.
Click Delete to delete the port and return to the IPS Services page.

Preferences
Use the IPS Preferences page (IPS > Preferences) to configure settings related to the Threat Suppression Engine and filtering performance.

This section discusses the following topics:

• “Reset Security Policy” on page 59
• “Configure the Threat Suppression Engine (TSE)” on page 60
• “Configure Adaptive Filter Settings” on page 61

Reset Security Policy
To restore IPS filters and associated settings to the factory default settings, use the Reset Security Policy option on the Preferences page.

CAUTION: The Reset Security Policy action restores all filters to their recommended Category Settings. You will lose any filter customizations made in the Security Profiles. You will also lose any user-created Action sets, rate limits, and traffic thresholds, and other user-configured options. You cannot undo this action.

1. From the LSM menu, click IPS > Preferences.
2. On the IPS Preferences page, click Reset in the Reset Security Policy section.
3. Click OK on the confirmation pop-up.
Configure the Threat Suppression Engine (TSE)

On the IPS Preferences page, you can configure global settings for the TSE in the Configure Threat Suppression Engine section.

1. From the LSM menu, click **IPS > Preferences**.
2. On the **IPS Preferences** page in the **Configure Threat Suppression Engine (TSE) table**, change the configuration parameters as required.
3. To configure **Congestion Percentage** and **Disable Time** for the disable logging feature, select **Disabled if congested in** in the **Logging Mode** field.
4. Click **Apply**.

Refer to the following table for a description of the TSE configuration parameters:

**Table 3 - 17: IPS Preferences: TSE Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Table Timeout (TCP)</td>
<td>Specifies the global timeout interval for TCP traffic on the connection table. For blocked streams in the connection table, this value determines the time interval that elapses before the blocked connection is cleared from the connection table. Before the timeout occurs, any incoming packets for that stream are blocked at the IPS device. After the connection is cleared (the timeout interval expires), the incoming connection is allowed until traffic matches another blocking filter. Blocked streams can also be cleared from the connection table manually from the Blocked Streams page (Events &gt; Managed Streams &gt; Blocked Streams).</td>
</tr>
<tr>
<td>Connection Table Timeout (non-TCP)</td>
<td>Specifies the global timeout interval for non-TCP traffic on the connection table.</td>
</tr>
<tr>
<td>Trust Table Timeout</td>
<td>Specifies the global timeout interval for the trust table. This value determines the time interval that elapses before the trusted connection is cleared from the trust table. After the connection is cleared, ??</td>
</tr>
<tr>
<td>Quarantine Timeout</td>
<td>Specifies the global timeout for the quarantine table. For quarantined hosts in the quarantine table, this value determines the time interval that elapses before the quarantined host is cleared from the quarantine table. After the quarantined host is cleared (the timeout interval expires), quarantined addresses may be automatically released, if that option is selected.</td>
</tr>
<tr>
<td>Asymmetric Network</td>
<td>Specifies whether the IPS device is configured for an asymmetric network. When asymmetric configuration is enabled, the IPS device will not see both sides of a TCP connection. This option is enabled by default.</td>
</tr>
</tbody>
</table>
Configure Adaptive Filter Settings

On the IPS Preferences page, you can configure the global settings for the adaptive filtering. At the filter level, you have the option to disable Adaptive Filter configuration so that a filter is never impacted by Adaptive Filter settings on the device. For details, see “Edit DV Filter Category Settings” on page 34.

You can view the effects of Adaptive Filter Configuration in the Ten Most Recent table, which displays the ten filters most recently affected by the Adaptive Filter. You can also manage the global Adaptive Filter configuration and the filter-level configuration. To change filter-level configuration, click on the linked name of a filter in the list. For more information, see “Adaptive Filter Report” on page 89.

1. From the LSM menu, click IPS > Preferences.
2. On the IPS Preferences page in the Adaptive Configuration Settings table, select the mode:
   - Automatic Mode: This setting enables the IPS device to automatically disable and log any defective filter.
   - Manual: This setting enables the IPS device to log any defective filter. However, the filter is not disabled.
3. Select the severity of the system log message that is automatically generated when a filter triggers the Adaptive Filter function.
4. Click Apply.

### Table 3 - 17: IPS Preferences: TSE Configuration Parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logging Mode</td>
<td>Configure settings to prevent traffic-related event notifications (such as those generated when a triggered filter is configured with a Block+Notify or Permit+Notify action set) from causing network congestion.</td>
</tr>
<tr>
<td></td>
<td>• Logging Mode determines whether logging is enabled/disabled when the network becomes congested. Always indicates that the system continues logging even if traffic is dropped under high load. Disable if congested indicates the logging will be disabled when the system reaches the specified congestion percentage.</td>
</tr>
<tr>
<td></td>
<td>• Congestion Percentage can be configured if the disable logging option is selected. This value specifies the amount of network congestion that can occur before the system disables logging functions.</td>
</tr>
<tr>
<td></td>
<td>• Disable Time specifies the amount of time (default is 10 minutes) that logging is disabled before the service is restarted. When the downtime expires, the system re-enables logging and displays the number of missed notifications.</td>
</tr>
<tr>
<td>Congestion Notification</td>
<td>Specifies whether alert messages will be sent when the overall device congestion exceeds the specified threshold.</td>
</tr>
</tbody>
</table>
IPS Filtering
Overview

The Events menu pages of the LSM allows you to monitor system performance and review traffic-related events. The menu provides the following options:

- **Logs** — View information on system events and traffic-related events triggered by IPS filters and policies (rate limits, traffic management, DDoS protection, and traffic threshold).
- **Managed Streams** — Review and manage traffic streams that have been blocked, rate-limited, trusted, or quarantined by IPS policies. You can also manually quarantine or release a quarantined IP address.
- **Health** — Review the current status and network performance of the IPS device. Information includes memory and disk usage statistics, status of the Threat Suppression Engine and the Ethernet ports, and throughput performance.
- **Reports** — View graphs showing information on traffic flow, traffic-related events, and statistics on triggered filters (attack, rate limit, traffic threshold, quarantine, and adaptive filter).

This chapter discusses the following subjects:

- “Logs” on page 64
- “Managed Streams” on page 72
- “Health” on page 80
- “Reports” on page 86
Logs

The Logs provide information on system events and traffic-related events triggered by the filters that are configured on the device. Each menu page also provides functions to manage the log files. Logs also indicate the interfaces through which administrators interacted with the system, such as the LSM, the CLI, or an SMS.

The IPS device maintains an historical log file and a current log file for each log. When the current log file reaches the default size (4MB), the log is de-activated and saved as the historical file, and a new log file is started as the current log. If a historical file already exists, that file is deleted. When the log is rolled over, the system generates a message in the Audit log. If you want to save log all data and create a backup, you can configure the system to offload log messages to a remote system log.

You can reset a log from its menu page, or use the Reset function available on the System Summary page.

**Note:** TippingPoint recommends that you have a compact flash card installed for log storage or designate a remote system log location.

This section discusses the following topics:

- “Alert Log” on page 65
- “Block Log” on page 66
- “Audit Log” on page 67
- “System Log” on page 68
- “Configure the Remote System Log Contact” on page 56
- “Viewing Logs” on page 69
- “Downloading a Log” on page 70
- “Resetting a Log” on page 70
- “Searching a Log” on page 71
Alert Log

The Alert log documents network traffic that triggers IPS filters configured with a Permit + Notify or Permit+Notify+Trace action set. Any user can view the log, but only administrator and super-user level users can reset the log.

To maintain a complete history of entries and provide a backup, you can configure the IPS device to send Alert Log entries to a remote syslog server from the Notification Contacts page. For more information, see the “Configure the Remote System Log Contact” on page 56.

An Alert log entry contains the following fields:

**Table 4-1: Alert Log Field Descriptions**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log ID</td>
<td>The system-assigned Log ID number.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>A date and time stamp in the format \texttt{YYYY-MM-DD HH:MM:SS}.</td>
</tr>
<tr>
<td>Severity</td>
<td>Indicates the severity of the triggered filter:</td>
</tr>
<tr>
<td></td>
<td>\begin{itemize}</td>
</tr>
<tr>
<td></td>
<td>\item 4: Critical</td>
</tr>
<tr>
<td></td>
<td>\item 3: Major</td>
</tr>
<tr>
<td></td>
<td>\item 2: Minor</td>
</tr>
<tr>
<td></td>
<td>\item 1: Low</td>
</tr>
<tr>
<td></td>
<td>\end{itemize}</td>
</tr>
<tr>
<td></td>
<td>When the log is downloaded, the severity is indicated with a number.</td>
</tr>
<tr>
<td>Filter Name</td>
<td>The name of the triggered IPS filter.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The name of the protocol that the action affects.</td>
</tr>
<tr>
<td>Virtual Segment</td>
<td>The virtual segment on which the alert occurred (such as 1A ==&gt; 1B).</td>
</tr>
<tr>
<td>Source Address</td>
<td>The source address of the triggering traffic.</td>
</tr>
<tr>
<td>Source Port</td>
<td>The source port of the triggering traffic.</td>
</tr>
<tr>
<td>Dest Address</td>
<td>The destination address of the triggering traffic.</td>
</tr>
<tr>
<td>Dest Port</td>
<td>The destination port of the triggering traffic.</td>
</tr>
<tr>
<td>Packet Trace</td>
<td>Indicates if a packet trace is available.</td>
</tr>
<tr>
<td>Hit Count</td>
<td>Number of packets that have been detected if packet trace is enabled.</td>
</tr>
</tbody>
</table>
Block Log

The IPS Block log documents packets that trigger IPS filters configured with any action that includes a Block + Notify or Block + Notify + Trace action, including Quarantine and TCP Reset action sets.

To maintain a complete history of entries and provide a backup, you can configure the IPS device to send IPS Block Log entries to a remote syslog server from the Notification Contacts page. For more information, see the "Configure the Remote System Log Contact" on page 56.

An IPS Block log entry contains the following fields:

Table 4 - 2: Block Log Field Descriptions

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log ID</td>
<td>The system-assigned Log ID number.</td>
</tr>
<tr>
<td>Date/Time</td>
<td>A date and time stamp in the format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>Severity</td>
<td>Indicates the severity of the triggered filter:</td>
</tr>
<tr>
<td></td>
<td>• 4: Critical</td>
</tr>
<tr>
<td></td>
<td>• 3: Major</td>
</tr>
<tr>
<td></td>
<td>• 2: Minor</td>
</tr>
<tr>
<td></td>
<td>• 1: Low</td>
</tr>
<tr>
<td></td>
<td>When the log is downloaded, the severity is indicated with a number.</td>
</tr>
<tr>
<td>Filter Name</td>
<td>The name of the triggered IPS filter.</td>
</tr>
<tr>
<td>Protocol</td>
<td>The name of the protocol that the action affects.</td>
</tr>
<tr>
<td>Virtual Segment</td>
<td>The virtual segment on which the alert occurred (such as 1A ==&gt; 1B).</td>
</tr>
<tr>
<td>Source Address</td>
<td>The source address of the triggering traffic.</td>
</tr>
<tr>
<td>Source Port</td>
<td>The source port of the triggering traffic.</td>
</tr>
<tr>
<td>Dest Address</td>
<td>The destination address of the triggering traffic.</td>
</tr>
<tr>
<td>Dest Port</td>
<td>The destination port of the triggering traffic.</td>
</tr>
<tr>
<td>Packet Trace</td>
<td>Indicates if a packet trace is available.</td>
</tr>
<tr>
<td>Hit Count</td>
<td>Number of packets that have been detected that matched the filter. Applies only if packet trace is enabled.</td>
</tr>
</tbody>
</table>
Audit Log

The audit log tracks user activity that may have security implications, including user attempts (successful and unsuccessful) to do the following:

- Change user information
- Change IPS, routing or network configuration
- Gain access to controlled areas (including the audit log)
- Update system software and attack protection filter packages
- Change filter settings

**Note:** Only users with Super-user access level can view, print, reset, and download the audit log.

To maintain a complete history of entries and provide a backup, you can configure the IPS device to send Audit Log entries to a remote syslog server from the Syslog Servers page. For more information, see the “Syslog Servers” on page 112.

An Audit log entry contains the following fields:

**Table 4 - 3: Audit Log Field Descriptions**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log ID</td>
<td>The system-assigned Log ID number.</td>
</tr>
<tr>
<td>Log EntryTime</td>
<td>A date and time stamp in the format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>User</td>
<td>The login name of the user who performed the audited action. The user listed for an event may include SMS, SYS, and CLI.</td>
</tr>
<tr>
<td>Access</td>
<td>The access level of the user performing the action</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address from which the user performed the action</td>
</tr>
<tr>
<td>Interface</td>
<td>The interface with which the user logged in: WEB for the LSM, CLI for the Command Line Interface. For system-initiated actions, SYS displays in this field.</td>
</tr>
<tr>
<td>Component</td>
<td>The area in which the user perform an action (LOGIN, LOGOUT and Launch Bar Tabs)</td>
</tr>
<tr>
<td>Result</td>
<td>The action performed or the result of a LOGIN or LOGOUT attempt</td>
</tr>
<tr>
<td>Action</td>
<td>The action performed as a result. For example, Log Files Reset.</td>
</tr>
</tbody>
</table>
System Log

The System Log contains information about the software processes that control the IPS device, including startup routines, run levels, and maintenance routines. System log entries can provide useful troubleshooting information if you encounter problems with your IPS device.

To maintain a complete history of entries and provide a backup, you can configure the IPS device to send System Log entries to a syslog server from the Syslog Servers page. For more information, see “Syslog Servers” on page 112.

Note: Users with any access level can view and print the system log, but only Administrator and Super-user level users can reset this log.

For information on Adaptive Filter messages, see “Configure Adaptive Filter Settings” on page 61.

System Log entries are only sent to the syslog server after the device has fully booted. During the boot sequence, entries cannot be sent because network ports are not yet enabled. When the boot sequence completes, the device sends a startup message to the syslog server.

A System log entry contains the following fields:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log ID</td>
<td>A system-assigned Log ID number.</td>
</tr>
<tr>
<td>Log Entry Time</td>
<td>A date and time stamp in the format YYYY-MM-DD HH:MM:SS.</td>
</tr>
<tr>
<td>Severity Level</td>
<td>Indicates whether the log entry is informational (INFO) or whether it indicates an error or critical condition (ERR or CRIT).</td>
</tr>
<tr>
<td>Component</td>
<td>Indicates which software component sent the message to the log.</td>
</tr>
<tr>
<td>Message</td>
<td>Text of the log entry.</td>
</tr>
</tbody>
</table>

Table 4 - 4: System Log Field Descriptions

CAUTION: Remote syslog, in adherence to RFC 3164, sends clear text log messages using the UDP protocol with no additional security protections. Therefore, you should only use remote syslog on a secure, trusted network to prevent syslog messages from being intercepted, altered, or spoofed by a third party.
Viewing Logs

On each log page, the functions available for the log are displayed at the top of the page. You can also access the log functions from the System Summary page. The following table describes these functions:

**Table 4 - 5: Log Functions**

<table>
<thead>
<tr>
<th>Function</th>
<th>Icon/Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td></td>
<td>To customize the display, specify the desired value in the Records per page field. To page through log entries, use the Navigation functions in the upper and lower left corners: &lt; &lt; Go to first page &lt; Go to previous page &gt; Go to next page &gt;&gt; Go to last page</td>
</tr>
<tr>
<td>Download</td>
<td>![icon]</td>
<td>Click the Download icon to download an electronic copy of the log or report. When you download some logs, the downloaded log file contains additional information that is not displayed in the LSM interface. For more information, see Appendix B, “Log Formats”.</td>
</tr>
<tr>
<td>Search</td>
<td>![icon]</td>
<td>Click the Search icon to search for an entry in the log or report.</td>
</tr>
<tr>
<td>Reset</td>
<td>![icon]</td>
<td>Use the Reset icon to clear a log of all current entries. The log will then begin compiling new information. Depending on your access level, this icon may not be available in the Audit and System logs.</td>
</tr>
</tbody>
</table>

See also:

- “Downloading a Log” on page 70
- “Searching a Log” on page 71
- “Resetting a Log” on page 70
- “Searching a Log” on page 71
Downloading a Log

The IPS device maintains two files for each log: a historical log file and a current log file. When the current log file reaches the default size (4MB), the log is de-activated and saved as the historical file, and a new log file is started as the current log. If a historical file already exists, that file is deleted. To save log data, download the log. In the LSM, the log view displays both current and historical log entries.

1. In the LSM, select the log that you want to download.
2. On the log page, click the Download icon. The Download Log page appears.
3. Verify that the Log Type dropdown list box has the correct log selected.
4. In the Log Entry section, specify one of the following criteria for which log entries will be included in the downloaded file:
   - All: Downloads all entries in the current and historical log files
   - Time Range: Downloads all entries within the specified dates and times.
   - ID Range: Downloads all logs with Log ID numbers within the specified range.
5. In the Options section, select one or both boxes for file format options:
   - Comma delimited format (csv): Saves the file as a comma-delimited file.
   - Open in browser: Opens the download file in the web browser.
6. Click Download.

Note: Downloaded logs provided more detailed information on each event than what is displayed in the LSM interface. For more information, see Appendix B, "Log Formats".

In the downloaded log, file entries are in a tab-delimited format with a line feed character terminating each line. Use WordPad or a spreadsheet application to view downloaded log files on a Windows workstation.

Resetting a Log

When you reset a log, the LSM starts a new log file beginning with the current date and time based on the system time. All previous information is permanently deleted. For record keeping, you may want to download the log before performing a reset. For more information, see "Downloading a Log" on page 70.

Note: Only Administrator and Super-user level users can reset the system log. Only Super-user level users can reset the audit log.

1. In the LSM, select the log that you want to reset.
2. Click Reset.
3. A confirmation message displays, prompting if you want to reset the log.
4. Click OK.
Searching a Log

The Alert, System, and Block logs provide a search function to help locate specific entries. The Audit log cannot be searched.

1. Select the log that you want to search and click the Search button at the top of the page.

In the Search Log page, specify the search criteria. The available criteria will vary depending on the log that you are searching.

- **All**: Searches all log entries.
- **Date Range**: Locates all logs between the specified dates and times.
- **Severity**: The severity includes low, minor, major, and critical events.
- **Filter Name**: The filter that triggered logged events.
- **Protocol**: The name of the protocol that the action affects.
- **Source Address**: The source address of the triggering traffic.
- **Source Port**: The source port of the triggering traffic.
- **Destination Address**: The destination address of the triggering traffic.
- **Destination Port**: The destination port of the triggering traffic.
- **Component**: Audit Log only. The type of event recorded by the Audit Log.

2. Choose the # of Results to Display from the drop-down box [optional].

3. Click Search.

Tip: When you enter filter names or IP addresses, you can enter partial names or addresses. For example you can enter the first few letters or numbers in a filter name, or the first few numbers of an IP address.
Managed Streams

The Managed Streams menu pages provide options to review and manage traffic streams that have been blocked or rate-limited by IPS policies. These events are captured by the Threat Suppression Engine (TSE), which uses a blend of ASICs and network processors to detect threats and anomalies in network traffic. There are two types of managed traffic streams:

- **Blocked streams**: Traffic streams detected and blocked based on filters configured with a Block action set.
- **Rate-Limited streams**: Traffic streams detected and rate limited based on filters configured with a Rate-Limit action set.
- **Quarantined**: Hosts and addresses that have been quarantined based on traffic that triggered a quarantine filter.
- **Trusted**: Traffic that has been trusted based on a trust action set.

This section discusses the following topics:

- “Blocked Streams” on page 73
- “Search Blocked Streams” on page 74
- “Flush Blocked Streams” on page 74
- “Rate Limited Streams” on page 75
- “Search rate-limited streams” on page 76
- “Flush rate-limited streams” on page 76
- “Quarantined Addresses” on page 77
- “Force IP Address into Quarantine” on page 77
- “Search quarantined addresses” on page 77
- “Flush quarantined addresses” on page 78
- “Trusted Streams” on page 78
- “Search trusted streams” on page 79
- “Flush trusted streams” on page 79

For more information about action sets, see “Action Sets” on page 50.
Blocked Streams

When traffic triggers an IPS filter that has been configured with a Block or Block+Notify action, traffic from the source IP address and port is blocked and an entry is added to the Blocked Streams page, based on the contact configuration in the action set. From the Blocked Streams page, you can:

- View and search for information on blocked streams
- Manually clear all or selected blocked stream connections

The Blocked Streams table displays up to 50 entries. Entries are added when the block event occurs. Entries are automatically removed when the connection times out based on the Connection Table timeout setting configured from the IPS Preferences page. The default timeout settings is 1800 seconds (30 minutes). You can manually remove an entry from the table with the Flush function, which unblocks the stream.

For each blocked traffic stream, the Blocked Streams page provides the following information.

Table 4 - 6: Blocked Streams Table

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Protocol used by the blocked connection.</td>
</tr>
<tr>
<td>Src/Dest Address</td>
<td>Source or destination IP address of the connection.</td>
</tr>
<tr>
<td>Port</td>
<td>Port of the connection.</td>
</tr>
<tr>
<td>Src/Dest Address</td>
<td>Source or destination IP address of the connection.</td>
</tr>
<tr>
<td>Port</td>
<td>Port of the connection.</td>
</tr>
<tr>
<td>Virtual Segment</td>
<td>The virtual port pair where traffic was blocked or rate-limited.</td>
</tr>
<tr>
<td>Reason</td>
<td>The filter link that details why the traffic connection stream was blocked. Click the link to display and manage the filter.</td>
</tr>
</tbody>
</table>
Search Blocked Streams

1. From the LSM menu, click Events > Managed Streams > Blocked Streams.

2. Enter search criteria for any of the following:
   - Protocol: The protocol for the connection: All, TCP, UDP, ICMP
   - Source or Destination Address: The traffic source or destination IP address
   - Source or Destination Port: The traffic source or destination IP port

   Entering “0” or “any” in the fields you do not want to specify allows you to search on any of the fields (combination or single).

3. Click Search.

To reset the search, click Reset.

Note: When you specify a source or destination IP address and port, ensure that the specified port number corresponds to the IP address.

Flush Blocked Streams

You can manually unblock all or selected streams using the Flush functions available on the Blocked Streams page.

Note: Flushing all blocked streams can cause temporary congestion.

To flush all blocked streams

1. From the LSM menu, click Events > Managed Streams > Blocked Streams.

2. Scroll to the bottom of the Blocked Streams page.

3. Click Flush All.

To flush selected blocked streams

1. From the LSM menu, click Events > Managed Streams > Blocked Streams.

2. Select the streams that you want to flush by clicking the check box next to the entry.

3. Scroll to the bottom of the Blocked Streams page.

4. Click Flush Selected.
Rate Limited Streams

When traffic triggers an IPS filter configured with a Rate Limit action set, traffic from the source IP and port is limited based on the rate limit settings. Traffic from the source IP address and port to the destination IP address and port remains rate-limited until the connection timeout period expires, or until the connection is manually terminated from the LSM.

From the Rate Limited Streams page, you can:

- View and search for information on rate-limited streams
- Manually terminate all or selected rate-limited stream connections

For more information about performing these tasks, see “Search rate-limited streams” on page 76 and “Flush rate-limited streams” on page 76.

The Rate Limited Streams table displays up to 50 entries. Entries are added when the rate-limit event occurs. Entries are automatically removed when the connection times out based on the Connection Table timeout setting configured from the IPS > IPS Preferences page. The default timeout setting is 1800 seconds (30 minutes). You can manually remove an entry with the Flush functions, which removes the rate limit from the stream.

The Rate Limited Streams table provides the following information:

Table 4 - 7: Rate Limited Streams Table

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Protocol used by the rate limited connection.</td>
</tr>
<tr>
<td>Src/Dest Address</td>
<td>Source or destination IP address of the connection.</td>
</tr>
<tr>
<td>Port</td>
<td>Port of the connection.</td>
</tr>
<tr>
<td>Src/Dest Address</td>
<td>Source or destination IP address of the connection.</td>
</tr>
<tr>
<td>Port</td>
<td>Port of the connection.</td>
</tr>
<tr>
<td>Virtual Segment</td>
<td>The virtual port pair where the stream is rate limited.</td>
</tr>
<tr>
<td>Reason</td>
<td>The filter link that details why the traffic connection stream was blocked. Click the link to display and manage the filter.</td>
</tr>
</tbody>
</table>
Events: Logs, Traffic Streams, Reports

Search rate-limited streams

1. From the LSM menu, click Events > Managed Streams > Rate Limited Streams.
2. Enter search criteria for any of the following:
   - **Protocol**: The protocol for the connection: All, TCP, UDP, ICMP
   - **Source or Destination Address**: The traffic source or destination IP address
   - **Source or Destination Port**: The traffic source or destination IP port
     Entering “0” or “any” in the fields you do not want to specify allows you to search on any of
     the 4 fields (in combination or singly).
3. Click **Search**.

To reset the search, click **Reset**.

Flush rate-limited streams

You can manually remove a connection from the table for all or selected streams using the Flush functions available on the Rate Limited Streams page.

**To flush all rate-limited streams**

1. From the LSM menu, click Events > Managed Streams > Rate Limited Streams.
2. Scroll to the bottom of the Rate Limited Streams page.
3. Click **Flush All**.

**To flush selected rate-limited streams**

1. From the LSM menu, click Events > Managed Streams > Rate Limited Streams.
2. Select the streams that you want to flush by clicking the check box next to the entry.
3. Scroll to the bottom of the Rate Limited Streams page.
4. Click **Flush Selected**.
Quarantined Addresses

When traffic triggers an IPS filter that has been configured with a Quarantine action, the host is quarantined and an entry is added to the Quarantined Addresses page, based on the contact configuration in the action set. From the Quarantined Addresses page, you can:

- Manually force an address into quarantine
- Search for quarantined addresses
- Manually release all or selected quarantined hosts

For more information about performing these tasks, see:

- “Force IP Address into Quarantine” on page 77
- “Search quarantined addresses” on page 77
- “Flush quarantined addresses” on page 78.

The Quarantined Address(es) table provides the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>IP address under quarantine.</td>
</tr>
<tr>
<td>Reason</td>
<td>The reason the IP address is under quarantine.</td>
</tr>
</tbody>
</table>

**Force IP Address into Quarantine**

**Note:** To force IP addresses into quarantine, you must have quarantine action sets defined. See “Configure an Action Set” on page 53.

1. From the LSM menu, click **Events > Managed Streams > Quarantined Addresses**.
2. Enter the IP address that you want to quarantine.
3. Click **Quarantine**. The address is added to the Quarantined Address(es) table.

**Search quarantined addresses**

1. From the LSM menu, click **Events > Managed Streams > Quarantined Addresses**.
2. Enter the IP address for which you want to search. *Are there wildcards?*
3. Click **Search**. The Quarantined Address(es) table is filtered to match the search terms.

To reset the search, click **Reset**.
Flush quarantined addresses

You can manually remove addresses from quarantine for all or selected addresses using the Flush functions available on the Quarantined Addresses page.

To flush all quarantined addresses

1. From the LSM menu, click Events > Managed Streams > Quarantined Addresses.
2. Scroll to the bottom of the Quarantined Addresses page.
3. Click Flush All.

To flush selected quarantined addresses

1. From the LSM menu, click Events > Managed Streams > Quarantined Addresses.
2. Select the addresses that you want to flush by clicking the check box next to the entry.
3. Scroll to the bottom of the Quarantined Addresses page.
4. Click Flush Selected.

Trusted Streams

When traffic triggers an IPS filter configured with a Trust action set, traffic from the source IP and port is recorded on the Trusted Streams page. From the Trusted Streams page, you can:

- View and search for information on trusted streams
- Manually clear all or selected trusted stream connections

For more information about performing these tasks, see “Search trusted streams” on page 79 and “Flush trusted streams” on page 79. For more information about the trust action, see “Configure an Action Set” on page 53.

The Trusted Streams table displays up to 50 entries. Entries are added when the trust action occurs. Entries are automatically removed when the connection times out based on the Trust Table timeout setting configured from the IPS > IPS Preferences page. The default timeout setting is 1800 seconds (30 minutes). You can manually remove an entry with the Flush functions, which removes the trusted stream from the table.
The **Trusted Streams** table provides the following information:

### Table 4-9: Trusted Streams Table

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Protocol used by the trusted connection.</td>
</tr>
<tr>
<td>Src/Dest Address</td>
<td>Source or destination IP address of the connection.</td>
</tr>
<tr>
<td>Port</td>
<td>Port of the connection.</td>
</tr>
<tr>
<td>Virtual Segment</td>
<td>The virtual port pair where the stream is rate limited.</td>
</tr>
<tr>
<td>Reason</td>
<td>The filter link that details why the traffic connection stream was trusted. Click the link to display and manage the filter.</td>
</tr>
</tbody>
</table>

#### Search trusted streams

1. From the LSM menu, click **Events > Managed Streams > Trusted Streams**.
2. Enter search criteria for any of the following:
   - **Protocol**: The protocol for the connection: All, TCP, UDP, ICMP
   - **Source or Destination Address**: The traffic source or destination IP address
   - **Source or Destination Port**: The traffic source or destination IP port
   Entering “0” or “any” in the fields you do not want to specify allows you to search on any of the 4 fields (in combination or singly).
3. Click **Search**.

The Quarantined Address(es) table is filtered to match the search terms.

To reset the search, click **Reset**.

#### Flush trusted streams

You can manually remove a connection from the table for all or selected streams using the Flush functions available on the Trusted Streams page.

**To flush all trusted streams**

1. From the LSM menu, click **Events > Managed Streams > Trusted Streams**.
2. Scroll to the bottom of the **Trusted Streams** page.
3. Click **Flush All**.
**Events: Logs, Traffic Streams, Reports**

*To flush selected trusted streams*

1. From the LSM menu, click **Events** > **Managed Streams** > **Trusted Streams**.
2. Select the streams that you want to flush by clicking the check box next to the entry.
3. Scroll to the bottom of the **Trusted Streams** page.
4. Click **Flush Selected**.

**Health**

The Health menu pages show the current status and network performance of the IPS device. The menu provides the following options:

- **Monitor**: View status and statistics for device and module health, performance and throughput
- **Performance**: View device throughput status and performance. Access the Performance Wizard which provides information on current device status and advice on fixing any issues the device is experiencing.
- **Port Health**: View information for each Ethernet port on the device including current configuration settings.
- **High Availability**: View information on current high availability status.

This section discusses the following topics:

- “Monitor” on page 81
- “Performance” on page 82
- “Port Health” on page 83
- “High Availability” on page 83
Monitor

Use the Monitor page (Events > Health > Monitor) to view and monitor device state and health. The Device Health table displays the current status of a variety of chassis components, including power modules, fans, temperature, and memory and disk space usage.

Table 4 - 10: Device Health

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>The component or resource being monitored. These components include the following:</td>
</tr>
<tr>
<td></td>
<td>• Power Supply Status</td>
</tr>
<tr>
<td></td>
<td>• Memory</td>
</tr>
<tr>
<td></td>
<td>• Disk system</td>
</tr>
<tr>
<td></td>
<td>• Disk user</td>
</tr>
<tr>
<td></td>
<td>• Disk ramLog</td>
</tr>
<tr>
<td></td>
<td>• Disk ramTemp</td>
</tr>
<tr>
<td></td>
<td>• Disk ramRO</td>
</tr>
<tr>
<td></td>
<td>• Temperature</td>
</tr>
<tr>
<td></td>
<td>• I2C buses</td>
</tr>
<tr>
<td></td>
<td>• Fans</td>
</tr>
<tr>
<td></td>
<td>• Voltage</td>
</tr>
<tr>
<td>State</td>
<td>The current operating status of the component or resource being monitored.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Normal</strong>: usage is at normal levels</td>
</tr>
<tr>
<td></td>
<td>• <strong>Major</strong>: usage has reached the major threshold setting specified for the device</td>
</tr>
<tr>
<td></td>
<td>• <strong>Critical</strong>: usage has reach the critical threshold setting specified for the device</td>
</tr>
<tr>
<td></td>
<td>To set the thresholds that trigger the Major and Critical states for memory and disk usage, go to <strong>System &gt; Thresholds</strong> page.</td>
</tr>
<tr>
<td>Graph</td>
<td>A bar graph depicting the current usage level of the component or resource.</td>
</tr>
<tr>
<td>Details</td>
<td>The units being measured in the graph. For example, the memory component displays the percentage of total available memory in use.</td>
</tr>
</tbody>
</table>
Performance

To view the current throughput performance of the device, click Events > Monitor > Performance. The Performance/Throughput table displays the following information:

Table 4 - 11: Performance/Throughput

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Component</td>
<td>The port being monitored.</td>
</tr>
<tr>
<td>State</td>
<td>The current operating status of the port.</td>
</tr>
<tr>
<td></td>
<td>• Normal: The port is active without errors</td>
</tr>
<tr>
<td></td>
<td>• Major: The port is active but has errors</td>
</tr>
<tr>
<td></td>
<td>• Critical: The port is waiting for traffic or usage in a stand-by mode</td>
</tr>
<tr>
<td></td>
<td>• Out-of-service: The port is not working or disabled</td>
</tr>
<tr>
<td></td>
<td>• Diagnostic: The port is running a diagnostic</td>
</tr>
<tr>
<td></td>
<td>• Inactive: The port is not in use or is disabled.</td>
</tr>
<tr>
<td>Graph</td>
<td>A bar graph depicting the current usage level of the port.</td>
</tr>
<tr>
<td>Details</td>
<td>Percentage of throughput used.</td>
</tr>
</tbody>
</table>

The System Performance Messages table appears below the Performance/Throughput table. This table provides information about current system performance. If the system is experiencing problems, the table displays messages indicating the cause of the problem and with suggested remedies.
**Port Health**

To view Port Health information for each port on the device, click **Events > Health > Port Health**. The Port Health table displays the following information:

**Table 4 - 12: Port Health**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>Port number, listed by segment.</td>
</tr>
<tr>
<td>Speed</td>
<td>Port speed.</td>
</tr>
<tr>
<td>Duplex</td>
<td>Indicates if the port is set to full or half for duplex.</td>
</tr>
</tbody>
</table>
| State  | A description of the current operation state of the port.  
- **Active**: The port is active without errors  
- **Out-of-service**: The port has been disabled.  
- **Active With Faults**: The port is enabled but disconnected.  
- **Degraded**: The port is enabled but inactive. |
| Info   | The current state of any SFP or XFP module attached to the port. |
| Link Status | Indicates if the link is down or up. |
| Media  | The port medium, which may be copper or fiber |
| Type   | The type of the port. |

**High Availability**

The High Availability page lists the current high availability status for the following High Availability features:

- Intrinsic Network High Availability
- Transparent High Availability
- Zero-Power High Availability

Some devices support the Smart ZPHA module in conjunction with the 10GbE segments. Users who have the Smart ZPHA module will see two entries under Zero Power High Availability:

- **External**: The external ZPHA module.
- **10GbE Segment**: The Smart ZPHA module. It is listed by the 10GbE segment name.
Intrinsic Network HA

Intrinsic Network HA (INHA) determines how the IPS device manages traffic on each segment in the event of a system failure. When the system fails, the device goes into Layer-2 Fallback mode and either permits or blocks all traffic on each segment, depending on the Layer-2 Fallback action setting for the segment. When the device is in Layer-2 Fallback mode, any traffic allowed through the device will not be inspected; it simply passes through the device.

A lack of reported errors or congestion through the TSE does not guarantee that the components receive correct and error-free traffic. The INHA monitors the TSE for several points of failure and applies failure detection logic against the system. All components for the INHA are checked for failure.

The IPS device performs the following checks to detect a failed condition and trigger a Layer-2 Fallback:

- Check back-pressure: Presence of back-pressure indicates packets are queued for processing. It indicates a failure if it does not process packets.
- Determine traffic requirements: If the IPS does not pass traffic, the ability to detect a failed TSE is more difficult. A minimum rate of traffic must pass through the IPS for best TSE-failure detection.
- Handle non-atomic nature of the data path: Packet pass through each component at different times and rates. The status of each component is determined independently of each other. INHA uses sampling to determine if the TSE is healthy.
- Check and transmit the inbound receive counters: Each component has receive counters incremented by packets received from the previous component. The component transmits these counters incremented as packets to the next component. These counters are the most accurate and most complicated way of detecting TSE health.
- Dropped packets exceeds threshold: If too many packets awaiting deep inspection are queued up, packets will be dropped.
- Memory lows: If available system memory is too low for proper operations.
- Various chip set errors: Represents possible hardware problems.

Each component also has a specific set of functions for failure checking.

You can view and configure the Layer-2 Fallback behavior for each segment from the Network Segments page (Network > Segments). The default setting for each segment is to permit all traffic. This setting is usually preferred by service providers because it prevents a device outage from becoming a network outage. However, for greater security, you may want to change the default the Layer-2 Fallback setting to block all to guarantee that no uninspected traffic enters the network.

You can view and manually change the current INHA state (normal or Layer-2 Fallback) from the High Availability menu page.
Transparent HA

Transparent High Availability allows the user to install two IPS devices in a redundant network configuration. Transparent HA keeps the devices in sync with each other so that if one experiences a system failure, the network flow can be routed to the other with no interruption in intrusion prevention services.

Note: Data may not reach the peer machine if “active” machines are under extremely heavy load.

Transparent HA requires you to configure two IPS devices with the same settings. Before you can configure the Transparent HA settings on a device, the devices must meet the following network setup and communication requirements:

- Each device must have a secure connection to the network and to the other device in the Transparent HA pair
- Both devices must have SSLv3 capability (HTTPS server enabled, which is the default setting) and be able to communicate on TCP port 9591.
- A device configured with Transparent HA can only connect and communicate with a partner configured to talk to other IPS devices configured with TRHA. In other words, both machines participating must point to each other.

CAUTION: A hijacked IPS or a rogue IPS that “steals” the IP address of a TRHA partner can communicate with a legitimate IPS.

You can configure the Transparent HA settings and manually enable or disable the feature from the device High Availability menu page. See “Configuring High Availability from the LSM” on page 109.

Note: If your system has two IPS devices communicating through Transparent HA, a change to the global timeout for the connection table at one IPS device will not propagate to the other IPS. You must make this change on each device accordingly.

Zero-Power HA

Zero-Power High Availability provides high availability through an external device or through a Smart ZPHA module. Some devices support the Smart ZPHA module in conjunction with the 10GbE segments. For detailed information about the Smart ZPHA module, refer to the TippingPoint Smart ZPHA Installation Guide.
Editing High Availability Configuration


2. Edit your High Availability settings as needed:
   - **Intrinsic Network HA**: Select **Normal** to handle traffic normally. Select **Layer-2 Fallback** to place the device in **Layer-2 Fallback** mode.
   - **Transparent HA**: Select the check box to enable Transparent HA. You must enter the IP address of the partner device that will process traffic when the current device is unavailable.
   - **Zero-Power HA**: Select **Normal** to handle traffic normally. Select **Bypass** to bypass the device.

3. Click **Apply** to apply the changes.

Reports

The **Reports** provide access to detailed information about the LSM system alert and traffic activity. Data for each report is gathered in real time. You can use the **Refresh** option on each report page to get the most current report information. On some reports, an **Animate Charts** option is available.

The following Reports are available:

- **Attacks**: Displays data on traffic that has been filtered by the device based on the Digital Vaccine filter configuration in a Security Profile.
- **Rate Limits**: Displays a bar graph showing the percentage of rate limit bandwidth used for each action set configured with a rate limit.
- **Traffic**: Displays traffic flow data categorized by transmission type, protocol, frame size, and port.
- **DDoS**: Displays the number of DDoS attacks on the system.
- **Quarantine**: Provides data on the number of hosts that have been quarantined over a selected time period.
- **Adaptive Filter**: Displays the global Adaptive Filter settings and a list of the 10 most recent filters impacted by adaptive filtering. You can also edit the Adaptive Filter settings from this report page.

This section discusses the following topics:

- “Attack Reports” on page 87
- “Rate Limit Reports” on page 87
- “Traffic Reports” on page 88
- “DDoS Report” on page 88
- “Quarantine Report” on page 89
- “Adaptive Filter Report” on page 89
**Attack Reports**

The **Attack Reports** page allows you to view data on traffic that has been filtered by the device based on the Security Profile configuration. This report reflects activity resulting from Digital Vaccine Filters.

Note: Additional information on attack filter events is available in the LSM logs. For more information, see “Logs” on page 64.

Traffic data is reported based on the view options you select. Each graph displays data based on the percentage of traffic affected by the filters.

- **Top Ten Filters**: Displays a bar graph of the top 10 attack filters. The graph also lists a packet count.
- **Severity**: Displays a bar graph of attacks categorized as Low, Minor, Major, and Critical. The graph also lists the number of attacks. The severity levels are assigned by the TippingPoint Digital Vaccine team and are included as part of the filter definition.
- **Action**: Displays the actions taken on filtered traffic. Traffic can be Invalid, Blocked, or Permitted. The graph also lists the number of packets processed with each action.
- **Protocol**: Displays attack traffic categorized by protocol (ICMP, ICMPv6, UDP, TCP, IPv4-Other, and IPv6-Other). The graph also lists the number of filtered packets for each protocol.
- **All**: Displays amount of all attack traffic reported by the virtual segment where the traffic was filtered.
- **Permit**: Displays amount of attack traffic permitted reported by virtual segments.
- **Block**: Displays amount of attack traffic blocked reported by virtual segment.

**Rate Limit Reports**

A rate limit action set defines the maximum amount of bandwidth available for traffic matching IPS filters that have the action set assigned. If two or more IPS filters use the same rate limit action set, then all packets matching these filters share the bandwidth. For each rate limit action set, the **Rate Limit Reports** page allows you to view the percentage of bandwidth consumed by rate-limited traffic graphed as a function of time. Data is reported based on the view options you select in the Rate Limit Reports page:

- **Rate Limit Action Set Name**: The list of available rate limit action sets is provided at the top of the rate limit table. To view the percentage of rate-limited bandwidth used for an action set, click on the action set name to update the report.
- **Reporting time interval**: select the time interval for the reporting period: Last 24 hours, Last 60 Minutes, Last 60 seconds.

Note: The Rate Limit report is only available if an Action Set has been configured with the Rate Limit action.

For more information about rate limit action sets, see “Action Sets” on page 50. For more information about rate-limited traffic streams, see “Rate Limited Streams” on page 75.
Traffic Reports

The traffic report provides profile data on the packets flowing through the device (permitted packets only). Traffic data is reported based on the view option you select on the Traffic Reports page:

- **Transmission Types**: The number of packets transmitted for each of the following transmission categories: Unicast, Broadcast, MultiCast, MAC control, FCS Errors, Align Errors
- **Protocol**: The number of packets transmitted by ICMP, ICMPv6, UDP, TCP, IPv4-Other, IPv6-Other, ARP, and Ethernet-Other
- **Frame size**: Traffic profile by frame size, by specified byte ranges
- **By Port**: Traffic profile by port

To update the traffic statistics over time, select the **Animate Charts** option. If this option is not selected, click the **Refresh Data** link to view the most current information.

DDoS Report

The DDoS report shows how often DDoS filters have been triggered over a selected time period. The display is based on the view options that you select on the DDoS Report page.

- **Rejected SYNs/sec and Proxied Connections/sec**: In the first drop-down menu, you can view the data by the total number of rejected SYNs per second or proxied connections per second. This data is listed by DDoS filter.
- **Time Period**: In the second drop-down, you can select parameters to view the reports over the following time periods:
  - 35 days
  - 24 hours
  - 60 minutes
  - 60 seconds
Quarantine Report

The Quarantine report provides data on the number of hosts that have been quarantined over a selected time period. The display is based on the view options that you select on the Quarantine Report page.

- **Hosts, Packets, or Pages**: In the first drop-down menu, you can select parameters to view the data by the total number of quarantined hosts, the number of packets blocked, source pages, and redirected pages.
- **Time Period**: In the second drop-down, you can select parameters to view the reports over the following time periods:
  - 35 days
  - 24 hours
  - 60 minutes
  - 60 seconds

Adaptive Filter Report

From the Configure Adaptive Filter Events Report page, you can:

- review and modify the global Adaptive Filter configuration
- view a list of the 10 most recent filters managed by adaptive filtering
- disable adaptive filter settings for an individual filter.

The Configure Adaptive Filter Events report page provides the following information:

**Table 4 - 13: TSE Adaptive Filter Configuration Details**

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Settings</td>
<td>The Settings table allows you to change the global system configuration for the Adaptive Filter function. For more information, see “Configure Adaptive Filter Settings” on page 61.</td>
</tr>
<tr>
<td>Ten Most Recent table</td>
<td>Displays the ten most recent filters managed by adaptive filtering.</td>
</tr>
<tr>
<td></td>
<td>• Filter Name: The name of the filter being managed by the Adaptive Filter function. Click on the name of the filter for more information.</td>
</tr>
<tr>
<td></td>
<td>• Filter State: Indicates if the filter is enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td>• Adaptive Filter State: Indicates if adaptive filtering is enabled or disabled for the filter.</td>
</tr>
<tr>
<td></td>
<td>• Functions: Actions that can be performed on the filter.</td>
</tr>
</tbody>
</table>

For more information about the Adaptive Filters, see “Configure Adaptive Filter Settings” on page 61.

To disable adaptive filtering on a single filter

To disable adaptive filtering on a single filter, click the filter’s name. On the Edit Filter page, click **Do not apply adaptive configuration settings to this filter**.
To change global adaptive filter settings

1. From the LSM menu, click IPS > Reports > Adaptive Filter.
2. On the Configure Adaptive Filter Events page, select the mode:
   - **Automatic Mode**: This setting enables the IPS device to automatically disable and log any defective filter.
   - **Manual**: This setting enables the IPS device to log any defective filter. However, the filter is not disabled.
3. Select the severity of the system log message that is automatically generated when a filter triggers the Adaptive Filter function.
4. Click **Apply**.
System

Overview

The System menu in the LSM provides options for managing TOS and Digital Vaccine packages, system configuration options, and access to external resources, such as syslog and email servers and remote management applications.

This chapter includes the following subjects:

- “Update” on page 92
- “Management Port” on page 101
- “Management Routing” on page 103
- “Time Options” on page 104
- “SMS/NMS” on page 106
- “High Availability” on page 108
- “Thresholds” on page 110
- “Email Server” on page 111
- “Syslog Servers” on page 112
- “Named Networks” on page 112
In the LSM, you can manage system software and digital vaccine filter packages from the Update pages. These pages are located under the System > Update menu.

- **Update Summary**: Lists the following information:
  - Device product code and serial number. The serial number can be used to create a TMC account, and may also be needed when you contact TippingPoint Technical Support.
  - Currently installed versions of the TOS, the Digital Vaccine, IP Reputation package (if applicable) and license package. A rollback icon indicates that there is at least one prior version of the IPS software on the device that you can rollback to. See “Rolling Back to a Previous TOS Version” on page 95.
  - Previously installed TOS versions. You can delete TOS software and Digital Vaccine versions installed on the device.
  - Any auxiliary DV packages that have been installed
- **Install Package**: Enables installation of TOS, DV, IP Reputation, or license packages.
- **Auto DV Update**: Enables configuration of automatic DV updates.
- **System Snapshot**: Enables creation and management of system snapshots.

The Update page provides the following information about the device and its software state.

This section discusses the following topics:

- “Managing Current TOS Software” on page 92
- “Viewing and Managing Current Digital Vaccine Filters” on page 96
- “System Snapshots” on page 99

## Managing Current TOS Software

You can download and install TOS updates from the System > Update > Install Package page.

When downloading and installing a software package, verify that the package you download is not larger than the listed amount of free space. An unpacked package may require more space than anticipated, depending on your device model, saved snapshots and rollback versions, and the size of the available update. To make sure the device has enough disk space, you can delete previously installed software images from the Update page.

This section discusses the following topics:

- “Updating the TOS Software” on page 93
- “Download a TOS Software Update” on page 94
- “Install a Software Update” on page 94
- “Rolling Back to a Previous TOS Version” on page 95
- “Delete a previously installed TOS software version” on page 96
Updating the TOS Software

When improvements or additions are made to the IPS system, TippingPoint releases a software update on the TMC Web site (https://tmc.tippingpoint.com). You can download and install updates from this site.

**CAUTION:** You must read the release notes posted with the TOS software update package on the TMC. The release notes contain information that may make the difference between a successful software update and an unsuccessful software update.

TOS updates are hitless by default, and the device continues to inspect traffic flow while the software is updated. You also have the option to place the device in Layer-2 Fallback mode during the software update. If the device is in Layer-2 Fallback mode, traffic will be permitted through the device without inspection. If this option is selected, Layer-2 Fallback applies to all segments, regardless of the individual segment settings.

When you perform a software update, your current configuration and filter settings are persisted forward and an archive copy of your current filter settings is saved. If you perform a software rollback in the future, any changes made to your filter settings after the update will not be preserved.

During a graceful shutdown, as during an update or reboot (in the LSM or command in the CLI), Packet Trace data may not be automatically flushed to disk. To guarantee Packet Trace data is flushed to disk, do the following:

- Click on any Packet Trace icon in the alert or block logs
- Click on the Packet Trace (TCPDUMP) icon

The update procedure takes approximately 30 minutes for the entire procedure, depending on your download speed. The following table provides a summary of the process with time estimates.

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Manual or Automatic</th>
<th>Estimated Time</th>
<th>Link Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Download the package</td>
<td>Manual</td>
<td>Varies</td>
<td>Up</td>
</tr>
<tr>
<td>2</td>
<td>Install the package</td>
<td>Manual</td>
<td>15-20 minutes</td>
<td>Up</td>
</tr>
<tr>
<td>3</td>
<td>Reboot the TippingPoint device</td>
<td>Automatic</td>
<td>5 minutes</td>
<td>Intrinsic Network HA</td>
</tr>
<tr>
<td>4</td>
<td>Commit and update the changes</td>
<td>Automatic</td>
<td>A few seconds</td>
<td>Intrinsic Network HA</td>
</tr>
</tbody>
</table>

In the Intrinsic Network High Availability (INHA) state, the links remain up, but inspection is bypassed. For more information about INHA, see "Intrinsic Network HA" on page 84.

**Note:** Traffic is inspected during a hitless update; however, during a hitless reboot, traffic is not inspected.
Download a TOS Software Update

1. Log into the LSM.
2. From the LSM menu, click System > Update > Install Package.
3. On the Install Package page under Step 1, click Threat Management Center to access the TippingPoint Threat Management Center.
4. Login to the Threat Management Center. If necessary, create an account from the login page.
5. From the top menu bar on the TMC home page, click Releases > Software > modeltype > modelnumber. The model number and type is available on the LSM home page.
6. Click on the software update that you want to download. On the Software Details page, review the information about the package.
7. Click the Download tab to download the package to your local system. Make sure to note the download location and the file size.

After you have downloaded the update, you can install it from the LSM Update page. For details, see “Install a Software Update” on page 94

Note: If you are installing an IP Reputation package or a license package, the procedure is similar. You must purchase the appropriate package and receive the download instructions from your TippingPoint representative.

Install a Software Update

Prior to installing the new software, backup any custom filters you have created and implemented. The update will overwrite these files.

When you perform an update of the software, the Update page displays a set of status messages. See “Log Formats” on page 145 for details.

CAUTION: During the LSM install, do not close the browser window or navigate off the Update page while the software installs.

1. Download a software update package from TMC.
2. If you are not already on the System > Update > Install Package, navigate to that page.
3. Verify available disk space in Step 2 on the TOS & DV Update page.
   A. If the update package that you downloaded is smaller than the requirement listed, proceed to Step 3.
   B. If the update package is larger than the number listed, delete older versions of the software to free disk space. For details see, "Delete a previously installed TOS software version” on page 96. After freeing disk space, return to the System > Update > Install Package page.
4. In **Step 3** enable one or both of the following options, if desired:

- **Enable High Priority**: Gives requests from the software update process the highest system priority until the update completes. However, the system does not give package installation processes priority over attacks. If an attack occurs during an update, the system will not give priority to the update process at that time.

- **Enable Layer-2 Fallback**: Places the device in Layer-2 Fallback while the software update takes place. If selected, all segments will be placed in L2FB.

5. In **Step 4**, click **Browse** to select the update package file that you downloaded from the Threat Management Center.

6. Click **Install** to install the software update.

When updating the IPS software, the progress bar may be interrupted by a pop-up message window. If this occurs, you will need to monitor the update process using the system log. If the system log does not show any errors during the update process, the IPS reboots when the update is complete.

When the installation completes, the IPS performs a soft reboot. After the reboot, you can log back in to the system.

**Note:** If you are installing an IP Reputation package or a license package, the procedure is similar. You must purchase the appropriate package and receive the download instructions from your TippingPoint representative.

### Rolling Back to a Previous TOS Version

A rollback operation reverts the currently running software version on your IPS device to a previous working version. The system retains the settings and configurations of your system. However, not all functionality may be available depending on the version of the TOS you rollback to.

**CAUTION:** If you perform a rollback, read the release notes for both the software version you are rolling back from and the software version you are rolling back to.

When you perform a TOS rollback, current configuration settings are preserved, but filter settings revert to the settings that were in effect when the rollback version was archived. Any filter changes made after the target rollback version are deactivated, including attack protection filter updates.

1. On the **System > Update > Update Summary** page in the **Current Installed Versions** table, click the **Rollback** icon in the **Functions** column for the TOS Software. A confirmation message displays.

   The IPS device deletes the current operating system files and reinstalls the previous operating system files. The **Update** page displays a set of status messages. When the installation completes, the device performs a soft reboot. See "[Log Formats](#)" on page 145 for details about the update status messages.

2. After the devices installs the previous TOS version, log back into the LSM.

To restore the operating system you rolled back from, you will need to perform a software update installation on your IPS device.
Delete a previously installed TOS software version

Deleting a previously installed TOS version frees disk space on the device. Once a TOS version is deleted, it is no longer available for rollback.

**CAUTION:** Unless the device is out of disk space, do not delete the previous TOS image that you were running. If the current TOS image becomes corrupted, you can roll back to the previous version as explained in “Rolling Back to a Previous TOS Version” on page 95.

1. On the **System > Update > Update Summary** page in the **Previous TOS Versions** table, review the list of previous versions and decide which is safe to delete.
2. Click the **X** icon in the **Functions** column for the TOS software package you would like to delete. A confirmation message displays.
3. Click **OK**.

Viewing and Managing Current Digital Vaccine Filters

You can download and install DV updates from the Install Package page, and configure automatic DV updates from the Auto DV Update page.

When downloading and installing a Digital Vaccine package, verify that the package you download is not larger than the listed amount of free space. An unpacked package may require more space than anticipated, depending on your device model, saved snapshots and rollback versions, and the size of the available update. To make sure the device has enough disk space, you can delete previously installed software images from the Update page.

This section discusses the following topics:

- “Updating the Digital Vaccine (Filters)” on page 97
- “Enable Auto Update for Digital Vaccine” on page 97
- “Manually Download a DV Update” on page 98
- “Manually Install a DV Update” on page 98
Updating the Digital Vaccine (Filters)
When new types of network attack are discovered, or when detection methods for existing threats improve, the Digital Vaccine team at the Threat Management Center (TMC) creates and releases new filters to add to your filter database. These filters are released as Digital Vaccine (DV) packages.

When a new DV package is available for download, the TMC team sends notifications to existing customers. You have two options to update the DV on your device:

- Configure the Auto DV option on your device so that the device checks for new DV packages and automatically updates the device as necessary.
- Manually download and install the DV package.

Note: You cannot rollback to a previous Digital Vaccine version. If you want to use a previous version of a Digital Vaccine, download an older version of the Digital Vaccine package from the TMC.

To make sure the device has enough disk space, you may need to delete previously installed software images from the Update page. For details, see "Delete a previously installed TOS software version" on page 96.

Enable Auto Update for Digital Vaccine
If AutoDV is configured, the system automatically checks the DV version when you open the Auto DV Update page. The status is listed in the Auto Update section. To perform an update immediately, click Update Now.

1. From the LSM menu, click System > Update > Auto DV Update.
2. Click the Enabled check box to enable the option.
3. Select the type of schedule that you want to use for the DV update process.
   - Periodic: Performs an update every number of days starting from a set day. The option includes a time to perform the update.
   - Calendar: Performs an update on a set day and time per week.
4. Set the update parameters.
5. Click Apply. To perform an update immediately, click Update Now.
Manually Download a DV Update

You can manually download the most current DV from the TippingPoint Threat Management Center, and then manually install the DV update.

1. From the LSM menu, click **System > Update > Install Package**.
2. On the Install Package page in Step 1, click **Threat Management Center** to access the TippingPoint Threat Management Center.
3. Login to the Threat Management Center. If necessary, create an account from the login page.
4. From the top menu bar on the TMC home page, click **Releases > Digital Vaccine** to display the list of digital vaccine filters available.
5. Click on the software update that you want to download. On the Software Details page, review the information about the package.

   **Note:** For DV packages, you cannot rollback to a previous version. To use a previous version, download that version from the TMC.

   6. Click the Download tab to download the package to your local system. Make sure to note the download location and the file size.

Manually Install a DV Update

1. Download a DV package from TMC.
2. If you are not already on the **System > Update > Install Package**, navigate to that page.
   - If the DV package is smaller than the required space, proceed to Step 3.
   - If the DV package is larger than the number listed, delete older versions of the software to free disk space. For details see, “Delete a previously installed TOS software version” on page 96. After freeing disk space, return to the TOS/DV Update page and repeat Step 2 and 3.
4. In Step 3 enable one or both of the following options, if desired:
   - **Enable High Priority**: Gives requests from the DV update process the highest system priority until the update completes. However, the system does not give package installation processes priority over attacks. If an attack occurs during an update, the system will not give priority to the update process at that time.
   - **Enable Layer-2 Fallback**: Places the device in Layer-2 Fallback while the DV update takes place.
5. In Step 4, click **Browse** to select the DV update package file that you downloaded from the Threat Management Center.
6. Click **Install** to install the DV update.

While the new file is loaded onto your IPS device, an Update Progress page displays the current status of the update. After the installation completes, you are returned to the Update page. The new version displays in the Version column of the Current Installed Versions table.
System Snapshots

From the Update > System Snapshots page, you can create, manage, restore and import local snapshots for your IPS device. System snapshots can be restored on the same software version on which they were created. After restoring a snapshot, the device will always restart.

Before taking a system snapshot, ensure that a correctly formatted compact flash card is available.

**CAUTION:** You can apply a single snapshot to multiple devices. However, applying the snapshot to devices managed by an SMS can cause a device ID conflict. Do not apply a snapshot to multiple devices when managed by SMS.

Do not perform an Update of your software while running a snapshot. The system may experience conflicts.

The System Snapshots page provides the following information.

<table>
<thead>
<tr>
<th>Column</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the snapshot.</td>
</tr>
<tr>
<td>Date</td>
<td>The date the snapshot was generated.</td>
</tr>
<tr>
<td>Software Build</td>
<td>The build number for the TOS software running when the snapshot was generated.</td>
</tr>
<tr>
<td>Digital Vaccine</td>
<td>The version number of the Digital Vaccine package running when the snapshot was generated.</td>
</tr>
<tr>
<td>Model Type</td>
<td>The model name of the device on which the snapshot was generated.</td>
</tr>
<tr>
<td>Functions</td>
<td>Icons representing functions to manage snapshots. The following functions are available:</td>
</tr>
<tr>
<td></td>
<td>• Delete a snapshot</td>
</tr>
<tr>
<td></td>
<td>• Restore a snapshot</td>
</tr>
<tr>
<td></td>
<td>• Import a snapshot</td>
</tr>
</tbody>
</table>

This section discusses the following topics.

- “Create a Snapshot” on page 100
- “Import a Snapshot” on page 100
- “Restore a Snapshot” on page 100
- “Export a Snapshot” on page 100
- “Delete a Snapshot” on page 100
Create a Snapshot

1. From the LSM menu, click System > Update > System Snapshots.
2. In the Create snapshot field, type a name for the snapshot.
3. Click Create.

Import a Snapshot

1. From the LSM menu, click System > Update > System Snapshots.
2. In the Import Snapshot field, click Browse to select the file to import.
3. Click Install. The selected snapshot uploads and displays in the list of snapshots.

Restore a Snapshot

When you restore a snapshot, you replace all current settings with those from the snapshot. After restoring a snapshot, the device will always restart

**CAUTION:** You can apply a single snapshot to multiple devices. However, applying the snapshot to devices managed by an SMS can cause a device ID conflict. Do not apply a snapshot to multiple devices when managed by SMS.

1. From the LSM menu, click System > Update.
2. Click the System Snapshots tab.
3. In the Function(s) column for the snapshot you want to restore, click (Restore).

Export a Snapshot

1. From the LSM menu, click System > Update.
2. Click the System Snapshots tab.
3. In the Current Snapshots table, locate the snapshot you want to export.
4. In the Function(s) column, click (Export) button. When you export a snapshot, you save the snapshot to a local directory to later import if needed.

Delete a Snapshot

1. From the LSM menu, click System > Update.
2. Click the System Snapshots tab.
3. Locate the snapshot you want to delete. Click the (Delete) icon.
Management Port

The Management Port is a separate network connection used to communicate with your TippingPoint IPS device. During the initial IPS setup, you configure the network setting for the Management Port via the serial console. After the IPS is installed, you can use the Management Port option in the LSM (System > Management Port) to review or modify the management port configuration.

You can manage the management port settings and reboot the IPS device through the Management Port page.

The Management Port page includes the following features and options:

Table 5-1: LSM Management Port Configuration Options

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reboot Device</td>
<td>Reboots the device.</td>
</tr>
<tr>
<td>Management Port Services</td>
<td>Manages the web and CLI access services. By default, these options are set to HTTPS and SSH.</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>The IP address used to connect to your TippingPoint device. Must be a valid IPv4 address on the network segment to which the device is connected, in the form xxx.xxx.xxx.xxx/xx. If the routing prefix size is not specified, the default is 24. TippingPoint recommends configuring the management port on the IPS to use a non-routed IP address from the RFC 1918 Private Address space. This helps to prevent direct attack on the management port from the Internet.</td>
</tr>
<tr>
<td>Default IPv4 Gateway</td>
<td>The gateway through which the TippingPoint device communicates with external network entities. Must be a valid IP address in the form xxx.xxx.xxx.xxx/xx. If the routing prefix size is not specified, the default is 24.</td>
</tr>
<tr>
<td>IPv6 Link-Local Address</td>
<td>The link-local IPv6 address for the device. This field is read-only.</td>
</tr>
<tr>
<td>IPv6 Auto</td>
<td>Indicates whether automatic IPv6 configuration is enabled on the device.</td>
</tr>
<tr>
<td>IPv6 Auto Address</td>
<td>If automatic configuration is enabled, the IPv6 address assigned by the router. This field is read-only.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>The IPv6 address used to connect to your TippingPoint device. Enter none if automatic configuration is enabled.</td>
</tr>
<tr>
<td>Default IPv6 Gateway</td>
<td>The IPv6 gateway through which the TippingPoint device communicates with external network entities. Enter none if automatic configuration is enabled.</td>
</tr>
<tr>
<td>Host Name</td>
<td>The host name of the device. Must be a valid host name on your network segment, with a maximum of 32 characters.</td>
</tr>
<tr>
<td>Host Location</td>
<td>Optional description of the location of the TippingPoint device, with a maximum of 32 characters.</td>
</tr>
<tr>
<td>FIPS Mode</td>
<td>Indicates whether FIPS mode is enabled or disabled.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The device serial number.</td>
</tr>
</tbody>
</table>
This section discusses the following topics:

- “Reboot the IPS” on page 102
- “Configure the Management Port” on page 103

### Reboot the IPS

1. In the Navigation pane, click **System > Management Port**.
2. Click the **Reboot device** button.
3. A confirmation message displays warning you to save all of your work prior to rebooting.
4. Perform any saves prior to the reboot.
5. Click **OK**.

---

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS Primary Server</td>
<td>The IP address of the Domain Name Service (DNS) which is consulted for IP address resolution. Must be a valid IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>DNS Secondary Server</td>
<td>The IP address of the backup or secondary DNS host. Must be a valid IPv4 or IPv6 address.</td>
</tr>
<tr>
<td>DNS Domain Name</td>
<td>The name of the domain to use when resolving host names. This name is concatenated to form a fully qualified internet host name.</td>
</tr>
<tr>
<td>Auto Negotiation</td>
<td>Indicates whether auto-negotiation is enabled on the device.</td>
</tr>
<tr>
<td>Line Speed</td>
<td>The management port line speed.</td>
</tr>
<tr>
<td>Current Line Speed</td>
<td>The current management port line speed setting.</td>
</tr>
<tr>
<td>Duplex Setting</td>
<td>The management port duplex setting.</td>
</tr>
</tbody>
</table>

---

**CAUTION:** You should not configure the TippingPoint IPS to run the HTTP or Telnet server during normal operations. HTTP and Telnet are not secure and a malicious party could intercept device user names and passwords.

**Note:** TippingPoint recommends using the port IP address filter feature to limit access to the management port. Refer to `conf t host` in the TippingPoint Command Line Interface Reference for more information.

**Note:** IPv6 options are disabled if IPv6 was not enabled during the initial setup. Refer to the TippingPoint Command Line Interface Reference for information about enabling IPv6 on the IPS. See also “Management Routing” on page 103.

**Note:** Making changes to the IPv4 and IPv6 addresses, Default IPv4 or IPv6 Gateway, Auto-Negotiation, Line Speed, and Duplex Setting may interrupt your LSM session.
Configure the Management Port

Making changes to the IPv4 address, IPv6 address, Default IPv4 Gateway, Default IPv6 Gateway, Auto-Negotiation, Line Speed, and Duplex Setting may interrupt your LSM session.

1. In the Navigation pane, click System > Management Port.
2. Edit the management port settings as needed.
3. Click Apply.

**Note:** TippingPoint recommends using the port IP address filter feature to limit access to the management port. Refer to `conf t host` in the TippingPoint Command Line Interface Reference for more information.

**Note:** If your IPS will communicate with devices on a different subnet, you may need to configure the management routing for this communication. You may have to define a route or gateway for SMS devices, time servers (for SNTP), email servers (for email alerts), and workstations (for remote access to the CLI or LSM). For details, see “Management Routing” on page 103.

Management Routing

Routing options enable communication with network subnets other than the subnet on which the Management Port is located. If your IPS will only communicate with devices on the local network subnet, you do not need to configure a management port route, regardless of whether you are using IPv4 or IPv6.

However, if you are using IPv4 and the IPS will communicate with devices that are not on the local IPv4 subnet or accessible through the default gateway, you must define the routes to these devices. The automatic configuration option is only available for IPv6.

If IPv6 automatic configuration is enabled on the Management Port page (see “Management Port” on page 101) and an IPv6 autoconfig router is present, IPv6 routing will be handled automatically, and you do not need to define additional IPv6 routes. If automatic configuration is disabled, you must add an IPv6 route to communicate with a device that is not on the local subnet and is not accessible through the default gateway.

1. In the Navigation pane, click System > Management Routing.
3. Type the Gateway IP address used by the IPS to communicate with the destination network.
4. Click Add.
Time Options

The IPS device uses the system time in log files. To ensure log file accuracy, facilitate log analysis, and establish predictable scheduling, configure the correct time zone and timekeeping mechanism before using the device in a live environment.

Use the Time Options page (System > Time Options) to configure the time zone and timekeeping mechanism for the IPS device:

- **Internal Clock**: Configures the device to keep time independently using its internal clock.
- **SNTP Server**: Configures the device to synchronize its internal clock by querying user-defined Simple Network Time Protocol (SNTP) servers.
- **Time Zone**: IPS logs are kept in Universal Time (UTC or Greenwich Mean Time). Use this option to configure the time zone so that log times are translated into local values when displayed.

This section discusses the following topics:

- “Internal Clock” on page 104
- “SNTP Server” on page 105
- “Time Zones” on page 105

Internal Clock

Your TippingPoint IPS contains an internal CMOS clock. By setting the internal clock time, you can set the device to keep time independently.

1. From the LSM, click System > Time Options.
2. Select Internal Clock.
3. To automatically populate the date and time settings, click Set Time to Local Browser Time.
   OR
   Type the Date and Time.
4. Click Apply.
SNTP Server

To keep system time for your TippingPoint IPS using a Simple Network Time Protocol (SNTP) server, you must define Primary and Secondary SNTP Servers. SNTP servers are central servers that keep time coordinated with a central atomic clock. SNTP servers help keep network time synchronized so that network events that occur on different hosts can be compared.

Be sure that you configure all SNTP clients (both TippingPoint IPS and other network devices) to use the same SNTP servers. Using the same SNTP servers will help ensure that event times from different network entities can be meaningfully compared.

**CAUTION:** Using external SNTP servers could possibly make your IPS susceptible to a man-in-the-middle attack. It is more secure to use an SNTP server on a local, protected network.

1. From the LSM menu click System > Time Options.
2. Select the SNTP Server option.
3. Enter the IP address for a Primary SNTP server.
4. Enter the IP address for a Secondary SNTP server.
5. Enter the Duration in minutes.
6. Enter the Offset in seconds.
7. Enter the Port for the server.
8. Enter the amount of seconds for a Timeout.
9. Enter the maximum amount of Retries for connecting.
10. Click Apply.

Time Zones

Use the Time Zone configuration option to specify the IPS time zone. The default time zone for the IPS device is Universal Time (UTC or Greenwich Mean Time). If you change the default, the LSM logs will display time data based on the specified time zone.

**Note:** Although the system logs are kept in Universal Time (UTC), the LSM will translate UTC time values into local time values for viewing purposes.

1. From the LSM menu, click System > Time Options.
2. Select the correct Timezone from the drop down list.
3. If desired, click the check box to Automatically adjust clock for daylight saving changes.
4. Click Apply.
SMS/NMS

The TippingPoint Security Management System (SMS) enables you to remotely monitor and manage IPS devices and perform the following tasks:

- View, manage and edit device configuration
- Review logs and reports.
- Configure virtual ports and security policy.
- Distribute the port and policy configuration to multiple IPS devices.

From an NMS, you can remotely monitor the events and system status of the IPS device. Configuring an NMS enables applications such as HP OpenView™ to monitor the IPS device.

When a device is under SMS management, the message (DEVICE UNDER SMS CONTROL) displays in red at the top of each page in the LSM and the SMS/NMS page displays the serial number and the IP address of the controlling SMS. In this state, you can view system configuration and status. However, you can only edit Authentication configuration.

This section discusses the following topics:

- “Configure SMS Information” on page 107
- “View or Configure NMS Information” on page 107
- “Disable/Enable SMS Management” on page 108

Note: Communication between the IPS device and the SMS or NMS is managed by the SNMP server, which provides access to interface counters and other statistics, configuration data, and general system information via the Simple Network Management Protocol (SNMP). Enable the SNMP server by selecting the SNMP V2 option during the SMS/NMS configuration process. If you disable this option, SMS and NMS functionality is also disabled.
Configure SMS Information

1. From the LSM menu, click System > SMS/NMS.
2. Enter an SMS Authorized IP Address/CIDR. The default value is *Any*, which means that any SMS can manage the device. To specify a range of IP addresses, enter an IP address block (10.100.230.0/24, for example). This allows any SMS on the specified IP subnet to manage the device.
3. Select SNMP V2 or SNMP V3.
4. Click **Apply**.

**Note:** SNMP notification contacts require SNMPv2, and will not work when SNMPv2 is disabled.

**Note:** If the SMS resides on a different IP subnet than the IPS device, you may need to configure the routing to that subnet. For details, see “Management Routing” on page 103.

If the IPS device has previously been managed by an SMS, the serial number, IP address, and port for SMS displays.

View or Configure NMS Information

You can add multiple NMS Trap destinations. The IPS device will send event and activity notifications to the specified destinations. For details on the information included in these notifications to the NMS, see the *TippingPoint IPS Third Party Management Guide* available on the *TippingPoint Documentation CD* or from the TMC.

1. From the LSM menu, click **System > SMS/NMS**.
2. Select SNMP V2 or SNMP V3. This selection will determine your NMS Trap options.
3. Enter the **NMS Community String**. The string can be 1-31 characters long.
4. Enter the NMS Trap information.
   • If SNMP V2 is selected, only the IP Address and Port are required.
   • If SNMP V3 is selected, you must also enter the Engine ID, Username, and Password, and you must select AES or DES encryption.
5. Click **Add to table below**.
6. Click **Apply**.

**Note:** SNMP notification contacts require SNMPv2, and will not work when SNMPv2 is disabled.
Disable/Enable SMS Management

1. From the LSM menu, click System > SMS/NMS.

2. If the device is currently being managed, remove the selection from the SMS Control: Enabled check box.

If the device is not currently under management and an SMS serial number and IP address display, click the SMS Control: Enabled check box to turn management control over to the specified SMS.

If the device has never been managed by an SMS (the Enabled check box is not available), you can start managing it by logging into an SMS system with an authorized IP address. (For details on configuring an authorized IP address, see “Configure SMS Information” on page 107.)

High Availability

IPS devices provide High Availability (HA) functionality as a failover mechanism to minimize network downtime in the event of a device failure. The High Availability feature allows you to view the current HA status and change the configuration as needed. Three types of High Availability mechanisms are available:

- Intrinsic Network HA (INHA) for individual device deployment.
- Transparent High Availability (TRHA) for devices deployed in a redundant configuration where one device takes over for the other in the event of system failure.
- Zero-Power High Availability, which provides high availability through an external device or through a Smart ZPHA module. Some devices support the Smart ZPHA module in conjunction with the 10GbE segments. Users who have the Smart ZPHA module will see two entries under Zero Power High Availability:

The High Availability page includes the following fields.

Table 5-2: High Availability Details

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Intrinsic Network HA  | • **State:** Enables you to manually change the HA state for the device. Selecting **Layer-2 Fallback** and clicking **Apply** triggers high availability. Traffic flowing through each segment on the device will be either blocked or permitted based on the segment configuration. Any permitted traffic will not be inspected. Select **Normal** to return the device to normal operation.  
  • **Current State:** Indicates the current Intrinsic Network HA state of the IPS device. In **Normal** state, the device is operating normally and inspecting traffic. In **Layer-2 Fallback** state, the device is in Layer-2 fallback mode, handling traffic on each segment based on the Layer-2 fallback action setting (**permit or block**) for the segment. Any traffic allowed through the device is not inspected. |

TippingPoint Local Security Manager User's Guide V 3.1
Configuring High Availability from the LSM

1. From the LSM menu, click **System > High Availability**.

2. Edit your High Availability settings as needed:
   - **Intrinsic Network HA**: Select **Normal** to handle traffic normally. Select **Layer-2 Fallback** to place the device in **Layer-2 Fallback** mode.
   - **Transparent HA**: Select the check box to enable Transparent HA. You must enter the IP address of the partner device that will process traffic when the current device is unavailable.
   - **Zero-Power HA**: Select **Normal** to handle traffic normally. Select **Bypass** to bypass the device.

3. Click **Apply** to apply the changes.

Compact Flash

The Compact Flash page displays the model number, serial number, revision number, and capacity of the compact flash card currently inserted in the device. To mount, unmount, or change the configuration of the compact flash card, you must use the command line interface. Refer to the entries for the `compact-flash` and `conf compact-flash` commands in the **TippingPoint Command Line Interface Reference V 3.1**.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Transparent HA  | • **Enabled**: Enables Transparent HA. If selected, you must specify the IP address for the other IPS device configured as the HA partner.  
  • **Partner IP Address**: Specifies the IP address of the other IPS device in the transparent HA pair.  
  • **Current State**: Indicates the current TRHA state.  
  • **Communication error**: Indicates that an error occurred during communication.  
  • **Latency**: Indicates that a warning occurred during communication. **Normal** indicates that the system is operating normally. |
| Zero Power HA   | • **Normal**: Indicates that the device is operating normally.  
  • **Bypass**: Indicates that ZPHA is enabled. |
Thresholds

Use the Thresholds page to configure the thresholds for the system settings that are reported on the System Summary and Monitor pages. See “System Summary” on page 20 and “Health” on page 80 for more information about those pages.

On the Thresholds page, you can specify the following settings:

- Disk Usage Threshold
- Memory Usage Thresholds
- Power Supply Monitoring: Turn on the power supply monitor feature. When this option is selected, a Power Supply Status indicator displays on the System Summary and Monitor (Events > Health > Monitor) pages to monitor the state of the power supplies for an IPS device.

Set disk usage and memory thresholds

When setting Disk and Memory usage thresholds, set the major threshold to a level that provides enough time to react before the situation is critical. For example, for disk usage, set a level where the disk is getting full, but is not so full that system activity is interrupted. The default value for both disk and memory usage is 90%. Set the critical threshold at a level that warns users before damage is about to occur. The default value for both disk and memory usage is 95%.

Note: TippingPoint recommends that you do not change these values from their defaults.

1. From the LSM menu, click System > Thresholds.
2. On the Thresholds page, specify the disk and memory thresholds.
   A. For Disk Usage Threshold, enter a numeric value for the Major Levels and the Critical Levels. Ensure that the value for the major level value is lower than the value for the critical level.
   B. For Memory Usage Threshold, enter a numeric value for the Major Levels and the Critical Levels. Ensure that the value for the major level value is lower than the value for the critical level.
3. Click Apply.

To reset the values to the default settings, click Reset to Defaults.
Email Server

Use the Email Server page to configure the default email settings that are used when a triggered IPS filter sends an email. After configuring the Email Server, configure email contact information from the Notification Contacts page (IPS > Action Sets, then select Notification Contacts). See “Notification Contacts” on page 54.

1. From the LSM menu, click System > Email Server.
2. On the Email Server page, type the Default To Email Address. This address displays in the To Email Address field when a user creates an email contact from the LSM.
3. Type the From Email Address.
4. This address is used as the Reply-To address for messages sent from the IPS device.
5. Type the From Domain Name, such as tippingpoint.com.
6. Enter the SMTP Server IP Address. The IPS device must be able to reach the SMTP server that will be handling the email notifications.
7. Enter a value for the Email Threshold (per minute). This limits the numbers of emails sent per minute. The default is 10 emails per minute.
8. Click Apply.

Email Threshold

By default, the system allows ten (10) email alerts per minute. On the first email alert, a one minute timer starts. The systems sends e-mail notifications until the threshold is reached. Any notifications received after the threshold is reached are blocked. After one minute, the system resumes sending email alerts. The system generates a message in the system log whenever email notifications are blocked.

Testing Email

When you are finished, you can click the Test Email button to test the email server configuration. The IPS will attempt to send an email message using the server defined in the default email settings. If the email fails to send properly, check for the following possible causes:

- Email server must be reachable from the IPS.
- Email server may not allow mail relaying. Make sure you use account/domain that the email server accepts.

For more information about sending emails from the IPS device, see “Create an Email or SNMP Notification Contact” on page 57.
Syslog Servers

To maintain and backup all log data from the IPS device, you can configure remote syslog servers for the System and Audit logs.

**Note:** You can also configure remote syslog servers for traffic-related event logging (Alerts and Blocks). For details, see “Configure the Remote System Log Contact” on page 56.

1. From the LSM menu, click **System > Syslog Servers**.
2. Select **Enable syslog offload** for each log you want to offload.
3. Type the IP address for the remote server.
4. Click **Apply**.

Tip: Be sure that the device can reach the remote system log server on your network. If the server is on a different subnet than the IPS management port, you may need to configure the routing to that subnet (see “Management Routing” on page 103).

For more information, see “Logs” on page 64.

Named Networks

Use the Named Networks page to assign names to IPv4 and IPv6 addresses. A network name acts as an alias in the LSM for the named IPv4 or IPv6 network, and in any list where the IP address would normally appear, the network name will appear instead. You can also enter the network name in any IP address field.

**Note:** Network names are presentation-only. Any configuration settings are associated with the IP address, and changing the network name does not change the configuration. For example, if the name of IP address 100.23.45.123 is changed from Corporate to Corporate-A, all configuration settings associated with IP address 100.23.45.123 are retained.
The Named Networks page includes the following features:

### Table 5-3: Named Network features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable named networks | Enables the display of named networks in the LSM.  
**Note:** Named networks can always be used, regardless of whether this option is selected.  
This option only toggles the LSM display of IP addresses. |
| Always show full octet/word | Controls the display of named networks when a named network prefix does not fall on an octet boundary in IPv4 or a word boundary in IPv6.  
**Example:** A user assigns the name `NamedNetwork` to IPv4 address `192.168.128.0/17`.  
When this option is enabled, the LSM displays the address `192.168.129.1` as `NamedNetworkIPv4:129.1`.  
When this option is disabled, the LSM displays the address as `NamedNetworkIPv4:1.1`. |
| Named Network table | Displays all named networks currently configured on the device. |

### Adding a Named Network

1. From the LSM menu, click **System > Named Networks**
2. Click **Add a New Named Network**.
3. Enter the network name and the IPv4 or IPv6 address.
4. Click **Save**. The new named network is added to the list.

See also: "Named Networks" on page 112.
License

The License page displays the current licensing information for the device and its associated TippingPoint services.

The Status table on the License page includes the following fields.

**Table 5-4: License Status**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feature</td>
<td>The name of the licensed feature or service:</td>
</tr>
<tr>
<td></td>
<td>- <strong>LICENSE</strong>: The default license for the TippingPoint device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>UPDATE TOS</strong>: The license enabling you to update the TOS on the device.</td>
</tr>
<tr>
<td></td>
<td>- <strong>UPDATE DV</strong>: The license enabling you to update the latest TippingPoint Digital Vaccine filters.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Auxiliary DV</strong>: An optional license for additional Digital Vaccine features.</td>
</tr>
<tr>
<td></td>
<td>- <strong>ReputationDV</strong>: An optional license for ReputationDV.</td>
</tr>
<tr>
<td>Status</td>
<td>The current license status.</td>
</tr>
<tr>
<td>Permit</td>
<td>Indicates whether the feature is currently enabled on the device.</td>
</tr>
<tr>
<td>Expiration</td>
<td>The date that the license expires.</td>
</tr>
<tr>
<td>Details</td>
<td>Additional information about the license.</td>
</tr>
</tbody>
</table>
Overview

The **Network** menu pages in the LSM enable you to view and modify the setup of the IPS device so that it can work within your network environment. The following menu options are available:

- **Segments**: view and manage segment configuration for Layer-2 Fallback (high availability) and link down synchronization.
- **Network Ports**: manage port configuration (auto-negotiation and line speed), disable/enable or restart a port.
- **Virtual Ports**: create and manage virtual ports that logically classify your network traffic by ports and VLAN IDs so that you can apply IPS filtering to traffic.
- **Virtual Segments**: create and manage virtual segments to further refine the network traffic classifications.
- **VLAN Translation**: enable translation of traffic between different VLANs or between VLAN and non-VLAN interfaces.
- **Network Tools**: review the types of traffic that your network is receiving.

This chapter discusses the following topics:

- “Segments” on page 116
- “Network Ports” on page 118
- “Virtual Ports” on page 121
- “Virtual Segments” on page 124
- “VLAN Translation” on page 126
- “Network Tools” on page 128
Segments

Use the Segments page to view segments on the IPS device. The TippingPoint IPS enables you to protect multiple network segments. Each segment is composed of a pair of ports on the IPS device; for example, ports 1A and 1B compose one segment. These two ports integrate the IPS into the network.

Segment configuration defines how the IPS device will handle traffic and port status. You can specify settings for the following options:

- **Intrinsic Network HA Layer-2 Fallback Action** determines if the device permits all traffic or blocks all packet transfers on that segment if the device goes into high availability.
- **Link-Down Synchronization**, allows you to configure the IPS to force both ports down on a segment when the device detects a link state of down on one of the ports. When Link-Down Synchronization is enabled, the IPS monitors the link state for both ports on a segment. If the link goes down on either port, both ports on the segment are disabled. This functionality propagates the link state across the IPS.

When Link-Down Synchronization is enabled, segment monitoring begins only after link up is detected on both ports. When Link-Down Synchronization disables the ports on a segment, two audit log messages are generated. The first message in the audit log corresponds to the port with the link down. The second message corresponds to the segment partner. Additionally, an error message is added to the system log indicating which port was detected with the link down, activating Link-Down Synchronization for that segment.

*Note:* In addition to the physical segments on the device, you can also configure virtual segments, a software representation of ports composed of two virtual ports (incoming and outgoing) that allows you to classify and filter traffic on the network by both physical port and VLAN ID.

From this page you can complete the following tasks:

- View current high availability and link-down synchronization for each network segment
- Edit HA settings for Layer-2 fallback and link-down synchronization

This section discusses the following topics:

- “Edit IPS Segment Page” on page 117.
- “Configure a Segment” on page 118
Edit IPS Segment Page

Use the Edit IPS Segment page to configure the high availability and link down synchronization settings for each segment.

The following segment configuration parameters are available:

**Table 6 - 1: Segment Configuration Parameters**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Segment Name</td>
<td>The segment name. By default the segment name corresponds to the ports on the device. For example, Segment 1 comprises ports 1A and 1B. You can edit the segment name to make it more meaningful. For example, if your LAN is connected to Segment 1, you may want to change the segment name to LAN.</td>
</tr>
<tr>
<td>Intrinsic HA</td>
<td>Indicates if traffic is permitted or blocked when the device goes into Layer-2 Fallback mode. For more information about high availability, see “High Availability” on page 108.</td>
</tr>
<tr>
<td>Link Down Synchronization</td>
<td>Indicates how the IPS device manages the ports on the segment when the device detects a link down on one of the ports.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Hub</strong>: The partner port is unaffected.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Breaker</strong>: The partner port is disabled. Both ports must be manually restarted.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Wire</strong>: The partner port is disabled, and is automatically restarted when the original link down is resumed.</td>
</tr>
<tr>
<td>Wait Time</td>
<td>When LDS is set to Breaker or Wire, this field indicates the length of time a port must be down before the partner port is also taken down. The default is one second. The wait time can be any value from 0 to 240 seconds.</td>
</tr>
</tbody>
</table>
Configure a Segment

1. From the LSM menu, click Network > Segments.
2. Click the name of the Segment you want to edit.
3. On the Edit IPS Segment page, enter or change the Segment Name.

   **Note:** Segment names can only include letters, numerals, underscores (_), and spaces.

4. Specify the Intrinsic Network High Availability (INHA) layer-2 fallback action:
   - **Block All** stops all packet transfer if the device goes into high availability.
   - **Permit All** permits all packet transfer in the event of a fallback.
5. For Link-Down Synchronization, select an option and enter a **Wait Time** between 0-240 seconds.
   - **Hub:** Partner port is unaffected.
   - **Breaker:** Partner port is disabled, and manual restart will be required.
   - **Wire:** Partner port is disabled, and is automatically restarted when the original link down is resumed.
   - **Wait Time:** When LDS is set to **Breaker** or **Wire**, the length of time a port must be down before the partner port is also taken down.
6. Click **Save**.

Network Ports

Use the Network Ports pages to perform the following tasks:

- View and edit current port configuration
- Disable/Enable Auto Negotiation
- Disable/enable ports
- Restart a port

**Tip:** You can view the current status and port configuration from the Port Health page. See "Port Health" on page 83 for more information.

You can configure high availability and link down synchronization settings for port pairs, or segments, from the Segments page. See "Configure a Segment" on page 118 for more information.

By default, the IPS device sets all ports to auto-negotiate. With this setting, the IPS port negotiates the highest line speed supported by both the IPS port and its link partner. TippingPoint recommends configuring both the IPS ports and the link partners to auto-negotiate because it is the best, most reliable way to establish and maintain links. However, if the IPS device cannot establish or maintain a
link when auto-negotiate is set, you may need to disable auto-negotiation and configure the line speed and duplex settings.

When configuring the ports, remember that both link partners must be configured with identical settings. If one port is configured to auto-negotiate, the other port must also be configured to auto-negotiate. If only one port is configured to auto-negotiate, the link may come up, but one or both partners may experience poor performance or RX errors.

The following table describes the port configuration parameters.

**Table 6-2: Port Configuration Parameters**

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The IPS port number.</td>
</tr>
<tr>
<td>Auto Negotiation</td>
<td>Indicates whether the port auto negotiates line speed or uses the line speed and duplex settings as a forced port configuration. By default, Auto Negotiation is enabled.</td>
</tr>
<tr>
<td></td>
<td>• If Auto Negotiation is enabled, the IPS device automatically negotiates the highest common speed and duplex that the IPS and the link partner both support.</td>
</tr>
<tr>
<td></td>
<td>• If Auto Negotiation is disabled, the manually-configured Line Speed and Duplex settings are used. You may want to disable auto-negotiation on some older networks if the IPS device is unable to establish or sustain the link with its partner.</td>
</tr>
<tr>
<td>Line Speed</td>
<td>Indicates the line speed setting for the port.</td>
</tr>
<tr>
<td>Duplex Setting</td>
<td>Indicates whether the port is set to full or half duplex</td>
</tr>
<tr>
<td>Media</td>
<td>Indicates whether the port is Copper or Fiber</td>
</tr>
<tr>
<td>Port Enabled</td>
<td>Indicates whether the port is currently enabled or disabled.</td>
</tr>
<tr>
<td>Restart</td>
<td>Select this check box to restart the port when you click <strong>Apply</strong>.</td>
</tr>
</tbody>
</table>

**Note:** When auto-negotiation is enabled, for example, 1000 Mbps line speed is only available for copper ports when auto-negotiation is enabled. When auto-negotiation is disabled, the line speed can only be set to 100 Mbps or 10 Mbps.

This section discusses the following topics:

- “Edit Port Configuration” on page 120
- “Disable a Port” on page 120
- “Restart a Port” on page 120
- “Correcting Port Link-Down Errors” on page 121
**Edit Port Configuration**

For more information about port settings, see Table 6-2, “Port Configuration Parameters,” on page 119.

After making port configuration changes, select the **Restart** option and click **Apply** to restart the port and ensure proper functioning of the device.

If you use a copper-fiber translator, disable auto-negotiation on the IPS before clicking the **Restart** button. Some translators do not support auto-negotiation. When the copper cable is pulled, these translators do not attempt to auto-negotiate with the device. The device driver will attempt to re-initialize the port several times before timing out and placing the port in an Out-of-Service mode.

1. From the LSM menu, click **Network > Network Ports**.
2. Set the **Auto Negotiation** option for the port you want to configure.
   - Deselecting **Auto Negotiation** enables configuration fields for Line Speed and Duplex Setting if the port supports custom configuration of these settings.
3. Edit **Line Speed** and **Duplex** settings as required.
4. Select the **Duplex** setting: **Full** or **Half**.
5. Check the **Restart** checkbox.

Click **Apply** to save the configuration and restart the port.

**Disable a Port**

1. From the LSM menu, click **Network > Network Ports**.
2. On the **Port Configuration** page, clear the **Port Enabled** checkbox.
3. Check the **Disable** checkbox.
4. Click **Apply** to save the configuration and restart the port.

**Restart a Port**

If you use a copper-fiber translator (such as Netgear), you will need to turn off auto-negotiation on the IPS before clicking the **Restart** button. Netgear does not support auto-negotiation. When the copper cable is pulled, Netgear does not attempt to auto-negotiate with the device. The device driver will attempt to re-initialize the port several times before timing out and placing the port in an Out-of-Service mode.

1. From the LSM menu, click **Network > Network Ports**.
2. Select the **Restart** option next to the port that you want to restart.
3. Click **Apply** to save the configuration and restart the port.
Correcting Port Link-Down Errors

If the IPS device has errors indicating that the ports are unable to establish link, check the connections on the device.

If you use a copper-fiber translator (such as Netgear) and it is disconnected or loose, the device driver will attempt to re-initialize the port several times before timing out and placing the port in an Out-of-Service mode. In addition, Netgear does not support auto-negotiation. When you remove the copper cable or the cable is loose, Netgear does not attempt to auto-negotiate with the IPS device.

1. From the LSM menu, click Network > Network Ports.
2. On the Port Configuration page, clear the Auto Negotiation checkbox for the port that is not working.
3. Click the Restart checkbox.
4. Click Apply to restart the port.

With auto-negotiation disabled, the port should reset.

Virtual Ports

Use the Virtual Ports page to complete the following tasks:

- View a summary of current configuration for all Virtual Ports.
- Create a Virtual Port.
- Change the name of a default virtual port.
- Edit the configuration for a custom virtual port.
- Delete a custom virtual port.

A Virtual Port is a logical section of the network that is associated with one or more physical ports and VLAN IDs. Virtual ports are used to classify and filter traffic on the network and help refine the settings in security and traffic management profiles.

By default, an IPS device is configured with virtual ports that represent each physical port pairing on the device. For example, paired ports 1A and 1B are virtual ports corresponding to physical ports 1A and 1B. The default configuration encompasses all traffic on the port with any VLAN ID. You can create custom virtual ports to apply filters traffic based on specific physical ports and VLAN tags.

For more information about profiles, see “Security Profiles” on page 24 and “Traffic Management Profiles” on page 41.
The following table describes the Virtual Port configuration parameters.

**Table 6-3: Virtual Port Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name used to identify the virtual port.</td>
</tr>
<tr>
<td>Description</td>
<td>An optional parameter to provide more detailed identification information about the virtual port.</td>
</tr>
<tr>
<td>Physical Ports</td>
<td>The number of the physical port assigned to the virtual port.</td>
</tr>
<tr>
<td>Ports/VLAN IDs</td>
<td>The VLAN ID in which the port is included. A VLAN ID of any spans across all physical ports.</td>
</tr>
<tr>
<td>CIDRs</td>
<td>The CIDRs associated with a virtual port.</td>
</tr>
<tr>
<td>Functions</td>
<td>Functions that you can perform on the virtual port.</td>
</tr>
</tbody>
</table>

This section includes the following topics:

- “Create a Virtual Port” on page 123
- “Edit a Virtual Port” on page 124

**Virtual Port Example**

The following figure illustrates a sample virtual port configuration on an IPS device with four ports.

**Figure 6-1: Configuring Virtual Ports using physical ports and VLANs**

In this example, the IPS device is configured with the four default ports: 1A, 1B, 2A, and 2B and two custom virtual ports: Marketing and Development. The default ports have the VLAN ID configured as ANY which means that traffic on any of the ports with any VLAN tag is classified the same. The custom virtual ports allow you to apply separate IPS filtering and policies to traffic with the specified VLAN tag on the specified ports.
Configuration Overview: Ports and Segments

The IPS has a default configuration so that the device can pass traffic in most network environments after it has been installed and configured. However, you may need to customize the configuration for your network. The following provides a list of common configuration steps.

1. Modify default settings for high availability and link down synchronization for physical segments.

2. Modify physical port default settings for auto-negotiation, line speed, duplex, and state (enable/disable).

3. Rename default virtual ports, or create custom ports to classify network traffic to be filtered by the IPS device.

4. After customizing virtual ports, you can configure the filters to monitor traffic on the ports from the IPS menu.

Create a Virtual Port

1. From the LSM menu, click **Network > Virtual Ports**.

2. Click **Create Virtual Port**. The Create Virtual Port page appears.

3. Enter the **Port Name** for the new virtual port.

4. If desired, enter a **Description**.

5. Select the **Physical Ports** that you want to include in the definition. To include all physical ports, select **Any**. To select multiple ports, hold down the CTRL key on a PC or the Command key on an Apple Mac.

6. If you want to include VLAN IDs in the virtual port definition, enter the VLAN IDs in the VLAN ID field. Enter multiple VLAN IDs as a comma separated list of numbers or ranges of numbers (such as 5,7,25-33, 35). The first number in a range must be less than the last number. VLAN IDs cannot be less than 1 or greater than 4094.

7. If you want to include CIDRs in the virtual port definition, enter the values in the format `xyz.x.x.x/xy`.

8. Click **Add to table below** to create the port and save the configuration.

**Note:** With tagged ports, you can add as many physical ports/VLAN IDs to a virtual port definition as you require. If you select a physical port and VLAN ID combination that is already assigned to another virtual port, the port configuration will display as invalid after you create it. To correct the problem, edit the port configuration to remove the overlapping port or VLAN ID. If you do not correct the problem, the invalid configuration will be deleted when the device reboots.
Edit a Virtual Port

1. From the LSM menu, click **Network > Virtual Ports**.

2. Click the **Edit** icon for the zone you want to edit. The virtual port configuration fields appear at the top of the table.

3. Edit the **Port Name** and **Description** if desired.

4. Select the **Physical Ports** that you want to include in the definition. To include all physical ports, select **Any**. To select multiple ports, hold down the CTRL key on a PC or the Command key on an Apple Mac.

5. If you want to include VLAN IDs in the virtual port definition, enter the VLAN IDs in the VLAN ID field. Enter multiple VLAN IDs as a comma separated list of numbers or ranges of numbers (such as 5,7,25-33, 35). The first number in a range must be less than the last number. VLAN IDs cannot be less than 1 or greater than 4094.

6. Click **Save** to create the port and save the configuration.

**Note:** With tagged ports, you can add as many physical ports/VLAN IDs to a virtual port definition as you require. If you select a physical port and VLAN ID combination that is already assigned to another virtual port, the port configuration will display as invalid after you create it. To correct the problem, edit the port configuration to remove the overlapping port or VLAN ID. If you do not correct the problem, the invalid configuration will be deleted when the device reboots.

Virtual Segments

Virtual ports may also be organized into virtual segments. A virtual segment is made up of any two virtual ports that may include CIDR specifications, and can have a security profile and traffic management profile applied to it. Virtual segments enable further management of VLAN traffic.

Virtual segments are saved on the IPS in a prioritized table, and security profiles and traffic management profiles are applied in order of priority. For example, if port 1A is assigned to two different virtual segments, the profiles that are assigned to the higher-priority segment will be applied to the traffic on that port before the profiles assigned to the lower-priority segment.
The following table describes the Virtual Segment configuration parameters.

**Table 6-4: Virtual Segment Configuration Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precedence</td>
<td>Use the icon in this column to drag and drop virtual segments into the desired precedence order. The topmost virtual segment has the highest precedence.</td>
</tr>
<tr>
<td>Incoming Virtual Port</td>
<td>The incoming virtual port for the virtual segment. See “Virtual Ports” on page 121.</td>
</tr>
<tr>
<td>Outgoing Virtual Port</td>
<td>The outgoing virtual port for the virtual segment.</td>
</tr>
<tr>
<td>Security Profile</td>
<td>The security profile applied to the virtual segment.</td>
</tr>
<tr>
<td>Traffic Management Profile</td>
<td>The traffic management profile applied to the virtual segment.</td>
</tr>
<tr>
<td>Functions</td>
<td>Click on the icons to delete an existing virtual segment or add a new one.</td>
</tr>
</tbody>
</table>

**Create a Virtual Segment**

1. From the LSM menu, click **Network > Virtual Segments**.
2. From the drop-down menus on the bottom line of the table, select the incoming and outgoing virtual ports.
3. Select the security profile and traffic management profile that you want to apply to the virtual segment.
4. Click **Add**.

**Delete a Virtual Segment**

1. From the LSM menu, click **Network > Virtual Segments**.
2. In the table, locate the virtual segment that you want to delete.
3. Click **Delete**.
VLAN Translation

The IPS VLAN translation feature enables the user to deploy an IPS on an aggregation or distribution switch and selectively inspect traffic based on the switch configuration. This feature translates traffic between different VLANs or between VLAN and non-VLAN interfaces.

The following diagram shows a sample deployment of an IPS on a network in which three VLANs connect to a central distribution switch. The traffic is routed from the switch to the IPS, which inspects the traffic, performs the translation tasks, and routes the inspected traffic back onto the network.

Figure 6 - 2: Network with VLAN Translation

The user can configure the aggregation switch to send traffic to the IPS on a selective basis, focusing inspection capacity on the VLANs where the need is greatest.

**Note:** Security policies are applied to the incoming VLAN ID only.

VLAN mappings must be unique, with one incoming VLAN paired with one outgoing VLAN. The IPS does not translate one-to-many VLAN mapping.
The following table describes the VLAN Translations configuration parameters.

**Table 6-5: VLAN Translations Parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming Port</td>
<td>The IPS virtual port through which incoming traffic arrives.</td>
</tr>
<tr>
<td>Incoming VLAN ID</td>
<td>The ID of the incoming VLAN.</td>
</tr>
<tr>
<td>Outgoing VLAN ID</td>
<td>The ID of the outgoing VLAN.</td>
</tr>
<tr>
<td>Auto-Reverse</td>
<td>Select this option to enable automatic reverse VLAN translation. This option is enabled by default.</td>
</tr>
</tbody>
</table>

The following table describes the parameters listed in the VLAN Translations table.

**Table 6-6: VLAN Translations Table**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Port</td>
<td>The IPS virtual port through which incoming traffic arrives.</td>
</tr>
<tr>
<td>Input VLAN</td>
<td>The ID of the incoming VLAN.</td>
</tr>
<tr>
<td>Output VLAN</td>
<td>The ID of the outgoing VLAN.</td>
</tr>
<tr>
<td>Output Port</td>
<td>The IPS virtual port through which outgoing traffic leaves.</td>
</tr>
<tr>
<td>Auto-Reverse</td>
<td>Indicates whether automatic reverse VLAN translation is enabled.</td>
</tr>
<tr>
<td>Function</td>
<td>Select this option to enable automatic reverse VLAN translation. This option is enabled by default.</td>
</tr>
</tbody>
</table>

**Create a VLAN Translation**

1. From the LSM menu, click **Network > VLAN Translations**.
2. From the drop-down menu, select the incoming virtual port.
3. Enter the Incoming and Outgoing VLAN IDs. IDs must be between 1 and 4094, inclusive.
4. Ensure the desired reverse translation option is selected.
5. Click **Add to table below**.
Network Tools

The Network Tools page includes the Traffic Capture feature. This feature enables you to capture a selection of traffic received by the device, including traffic that triggers filters and traffic that does not trigger any filters. You can capture up to 10,000 packets or 10 MB (10,000,000 bytes) of traffic. The traffic capture files are saved on the external compact flash card.

The following table describes the Traffic Capture configuration parameters.

Table 6-7: Traffic Capture Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filename</td>
<td>The name under which you want to save the traffic capture file. If you do not specify a name, the file will be saved with a default name of the date and time at which the capture was initiated, in the format YYYYMMDD-HHMMSS.pcap.</td>
</tr>
<tr>
<td>Max Packets</td>
<td>The number of packets at which the traffic capture will stop. The default is 100.</td>
</tr>
<tr>
<td>Max File Size</td>
<td>The capture file size at which the traffic capture will stop. The size is defined in bytes. The default is 1,000,000.</td>
</tr>
<tr>
<td>Virtual Segment</td>
<td>The virtual segment on which you want to capture traffic. The default is all defined virtual segments.</td>
</tr>
<tr>
<td>Expression</td>
<td>Enables you to refine the types of packets that are captured. See &quot;Traffic Capture Expressions&quot; on page 129.</td>
</tr>
</tbody>
</table>

The following table describes the parameters listed in the Traffic Capture table.

Table 6-8: Traffic Capture Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Date on which the traffic capture was taken.</td>
</tr>
<tr>
<td>Time</td>
<td>Time at which the traffic capture was taken.</td>
</tr>
<tr>
<td>Filename</td>
<td>The names of any traffic capture files currently saved on the device.</td>
</tr>
<tr>
<td>Function(s)</td>
<td>Click on the icons to download or delete a traffic capture file.</td>
</tr>
</tbody>
</table>
Starting a Traffic Capture

1. From the LSM menu, click **Network > Network Tools**.
2. Specify the required parameters in the Traffic Capture Details section.
3. Enter an expression, if desired.
4. Click **Start**.

The traffic capture will start immediately, and will stop when the specified thresholds are reached or when you click **Stop**.

**Note:** By default, only IPv4 traffic is captured. If you want to capture IPv6 traffic, include the string `ip6` in the Expression field. IPv4 and IPv6 traffic cannot be captured at the same time.

Traffic Capture Expressions

Traffic capture expressions are used to narrow down the types of traffic that are captured. These expressions are similar in structure to TCPDUMP expressions. The following parameters are permitted:

- **ip**: IPv4 traffic. By default, only IPv4 traffic is captured.
- **ip6**: IPv6 traffic.
- **proto**: designates the protocol of captured traffic. Can be an explicit number or `tcp`, `udp`, or `icmp`.
- **src** and **dst**: specifies the source or destination of the traffic. Can be applied to both host and port.
- **host**: designates a host IP address. IPv4 and IPv6 addresses are supported, as is CIDR format.
- **port**: designates a port. You must specify a port number.

Parameters can be concatenated with the operator `&`. The `or` operator cannot be used.

**Examples**

To capture only TCP traffic, enter the following in the Expression field:

```
ip proto tcp
```

To capture only TCP traffic on port 63, enter the following:

```
ip proto tcp & src port 63
```
7

Authentication

Overview

Use the LSM Authentication pages enable administrators to create and manage user accounts, set user account preferences, and manage X.509 certificates.

This chapter includes the following subjects:

- “User List” on page 132
- “Preferences” on page 136
- “X.509 Certificates” on page 138
User List

Use the User List page to view the users currently configured on the device. The User List page provides the following information about the users:

<table>
<thead>
<tr>
<th>Heading</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>The user name.</td>
</tr>
<tr>
<td>Access Level</td>
<td>The access level granted to the user.</td>
</tr>
<tr>
<td>Password Expiration</td>
<td>The number of days remaining before the user's password expires.</td>
</tr>
<tr>
<td>State</td>
<td>Indicates whether the user account is enabled or disabled.</td>
</tr>
<tr>
<td>Function(s)</td>
<td>Functions that you can perform on the user account.</td>
</tr>
</tbody>
</table>

This section discusses the following subjects:

- “User Accounts” on page 132
- “Access Level” on page 132
- “Username and Password Requirements” on page 133
- “Create a New User Account” on page 134
- “Changing Passwords” on page 135

User Accounts

A User account provides access to the TippingPoint Operating System (TOS) to manage IPS devices through the LSM web interface or from the Command Line Interface (CLI). The management functions available to a user are determined by the account security level configured on the account. Accounts can only be defined in the embedded TOS user database on the IPS.

Access Level

You can configure one of three access levels for each user account:

- **Operator** — Base level administrator user who monitors the system and network traffic
- **Administrator** — Enhanced administrator user who can view, manage, and configure functions and options in the system
- **Super User** — Administrator user who has full access to all LSM and CLI functions
The following table summarizes the functions available to users based on the assigned Access Level (Operator, Administrator, or Super-user) assigned to their user account.

### 7 - 1: LSM Functions available to TOS Users based on Access Level

<table>
<thead>
<tr>
<th>Functional Area</th>
<th>Operator</th>
<th>Administrator</th>
<th>Super-user</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPS/Quarantine</td>
<td>view</td>
<td>all</td>
<td>all</td>
</tr>
<tr>
<td>Network</td>
<td>view</td>
<td>all</td>
<td>all</td>
</tr>
<tr>
<td>System</td>
<td>view</td>
<td>all</td>
<td>all</td>
</tr>
<tr>
<td>Events/Logs</td>
<td>view all except Audit log</td>
<td>view all except Audit log</td>
<td>all</td>
</tr>
<tr>
<td>Update</td>
<td>view</td>
<td>all</td>
<td>all</td>
</tr>
<tr>
<td>Configure</td>
<td>view</td>
<td>all except system time</td>
<td>all</td>
</tr>
<tr>
<td>Admin</td>
<td>• change own password • view system log</td>
<td>• change own password • view system log</td>
<td>all, including • change Idle Timeout • change Password Expiration</td>
</tr>
<tr>
<td>Help</td>
<td>view</td>
<td>view</td>
<td>view</td>
</tr>
</tbody>
</table>

### Username and Password Requirements

Restrictions on username and password values for user accounts are determined by the Security Level preference setting configured on the Preferences page. Username and password requirements are the same for local users and TOS users. There are three possible security levels available on the IPS:

- **Level 0:** User names and passwords are unrestricted.
- **Level 1:** Names must be at least 6 characters long; passwords at least 8.
- **Level 2:** In addition to level 1 restrictions, passwords must contain:
  - at least 2 alpha characters
  - at least 1 numeric character
  - at least 1 non-alphanumeric character

The default security level preference is **Maximum Security Checking.**
The following table provides examples of valid usernames and passwords based on the default setting for username/password Security Level (Maximum Security Checking).

Table 7 - 2: Login and Password Name Examples

<table>
<thead>
<tr>
<th>Security Level</th>
<th>Valid Login Names</th>
<th>Valid Passwords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0</td>
<td>fredj</td>
<td>mypass</td>
</tr>
<tr>
<td>Level 1</td>
<td>fjohnson</td>
<td>mypassword</td>
</tr>
<tr>
<td>Level 2</td>
<td>fjohnson</td>
<td>my-pa55word</td>
</tr>
<tr>
<td></td>
<td>fredj123</td>
<td>my-b1rthday</td>
</tr>
<tr>
<td></td>
<td>fredj-123</td>
<td>myd*g'snam3</td>
</tr>
<tr>
<td></td>
<td>fredj-*123</td>
<td></td>
</tr>
</tbody>
</table>

See “User List” on page 132.

Create a New User Account

Only a user with Super-user access level can create a user account. The user name and password must conform to the security level on the device:

- **Level 0**: User names and passwords are unrestricted.
- **Level 1**: Names must be at least 6 characters long; passwords at least 8.
- **Level 2**: In addition to level 1 restrictions, passwords must contain:
  - at least 2 alpha characters
  - at least 1 numeric character
  - at least 1 non-alphanumeric character

1. From the LSM menu, click Authentication > User List.
2. Click Create A New User. The Create User screen appears.
3. Enter a Username.
4. Select the Access Level for the account
   - Operator
   - Administrator
   - Super User.
5. Enter a Password.
6. Verify the password by re-entering it in Confirm Password field.
7. Click Create.
Changing Passwords

All TOS users can change the password on their own account. Only users with super user access can change passwords on any account. The password must conform to the security level on the device:

- **Level 0**: Passwords are unrestricted.
- **Level 1**: Passwords must be at least 8 characters long.
- **Level 2**: In addition to level 1 restrictions, passwords must contain:
  - at least 2 alpha characters
  - at least 1 numeric character
  - at least 1 non-alphanumeric character

1. From the LSM menu, click Authentication > User List.
2. On the User List page, click your Username.
3. On the Edit User page, select the Change Password check box.
4. Enter your new Password.
5. Verify the password by re-entering it in Confirm Password.
6. Click Save.
Preferences

From the Preferences page on the Authentication menu, TOS users with administrator or super user security level can configure preferences to manage the security settings that affect user account access and session management.

Tip: Session timeouts and password expiration periods may be covered in your company’s information security policy. Consult your security policy to be sure you configure these values appropriately.

The following table provides information on the security preferences parameters.

Table 7 - 3: Authentication: General User Preferences

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Idle Timeout</td>
<td>Time (in minutes) that can elapse with no user activity before the LSM logs out account access.</td>
</tr>
<tr>
<td>Page Refresh Time</td>
<td>The time period for the Auto Refresh option available on pages that have dynamic content, such as the System Summary page, Log pages, and Health page. If the option is enabled on a page, a countdown timer (starting with the value of Page Refresh Time) is started as soon as the page is opened. When the countdown expires, the page automatically refreshes.</td>
</tr>
</tbody>
</table>

Table 7 - 4: Authentication: TOS User Preferences

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Security Level      | Determines the length and complexity requirements for passwords. The following options are available:  
  • No Security Checking (Level 0): Usernames cannot have any spaces. Passwords are not required.  
  • Basic Security Checking (Level 1): User names must be 6-32 characters long; passwords must be 8-32 characters long.  
  • Maximum Security Checking (Level 2): In addition to the Basic requirements, passwords must be 8-32 characters long and contain at least one numeric character and one non-alphanumeric character (special characters such as ! ? and *). This is the default setting. |
| Password Expiration | Specifies how frequently users are required to change their passwords. TippingPoint recommends that password expiration periods should be a minimum of 30 days and maximum of 90 days. |
Table 7 - 4: Authentication: TOS User Preferences

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Expiration Action</td>
<td>Determines what action the system takes in response to a password expiration event. The following options are available: • Force user to change the password when it expires • Notify user of expiration. If this option is selected, the system notifies the user 5 days before the expiration occurs and at each subsequent login prompting the user to change the password before accessing the LSM. • Disable the account.</td>
</tr>
<tr>
<td>Max Login Attempts</td>
<td>Number of failed login attempts allowed before the system takes the action specified in the Failed Login Action field.</td>
</tr>
<tr>
<td>Failed Login Action</td>
<td>The action the system takes when the Max Login Attempt count has been exceeded. The following options are available: • Lockout Account. For this option, specify a Lockout Period. • Disable Account • Audit Event. This option creates an entry in the Audit log documenting the failed login attempt.</td>
</tr>
<tr>
<td>Lockout Period</td>
<td>If Lockout Account is selected as the Failed Login Action, this value determines the duration of the lockout.</td>
</tr>
</tbody>
</table>

**Set User Preferences**

If the fields on the Preferences page are read-only, your account does not have the required security access to edit the preferences. You must have an account with Administrator or Super-User access.

1. From the LSM menu, click Authentication > Preferences. The Preferences page appears.
2. Change the values as desired.
3. Click Save.
X.509 Certificates

Use the X.509 Certificates page to add X.509 certificates to the IPS. The IPS supports the following certificates:

- Certificate Authorities (CA) in PEM or DER format
- Certificate Revocation Lists (CRL) in PEM or DER format
- Multiple PEM certificates contained in a single file

The IPS uses the uploaded X.509 certificate to check any incoming certificates when the user connects to the LSM.

- If the incoming certificate is not yet valid, has expired, has been revoked, or is otherwise invalid the IPS logs an error in the system log and blocks the connection.
- If the incoming certificate is valid but has an unknown issuer, is self-signed, or includes the wrong purpose, the IPS permits the connection, but logs a warning in the system log.
- If the incoming certificate is valid and has a known issuer, the IPS completes the connection and does not record any errors in the system log.

Certificates may be obtained from or signed by a third party. You can also use self-signed certificates.

This section includes the following topics:

- “Import a CA Certificate” on page 138
- “Import a CRL Certificate” on page 138

Import a CA Certificate

1. Go to Authentication > X.509 Certificates.
2. In the File to Import field, click Browse and select the CA certificate you want to install.
3. Click Import.

The certificate is displayed in the Current Certificate Authorities table.

Import a CRL Certificate

1. Go to Authentication > X.509 Certificates.
2. In the File to Import field, click Browse and select the CRL certificate you want to install.
3. Click Import.

The certificate is displayed in the Current Certificate Authorities table.
Third-Party Licensing

This appendix includes all third-party licensing information.

Open Source Software

The following open source software used by the TOS requires that the full text of the license be published with the user documentation.

**gSOAP**

Part of the software embedded in this product is gSOAP software.

Portions created by gSOAP are Copyright (C) 2001-2004 Robert A. van Engelen, Genivia inc. All Rights Reserved.

THE SOFTWARE IN THIS PRODUCT WAS IN PART PROVIDED BY GENIVIA INC AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.”

**OpenSSH**

TippingPoint Core Controller uses a derivative of OpenSSH.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.
OpenSSH contains no GPL code.

1) Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland. All rights reserved

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "http://www.cs.hut.fi/crypto".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2) The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED `AS IS' AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com>
3) ssh-keyscan was contributed by David Mazieres under a BSD-style license.

Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>.

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5) One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.


The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6) Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

- Markus Friedl
- Theo de Raadt
- Niels Provos
- Dug Song
- Aaron Campbell
- Damien Miller
- Kevin Steves
- Daniel Kouril
- Wesley Griffin
- Per Allansson
- Nils Nordman
- Simon Wilkinson

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenBSD: LICENCE,v 1.19 2004/08/30 09:18:08 markus Exp

**zlib.h General Purpose Compression Library**

zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly [jloup@gzip.org](mailto:jloup@gzip.org) Mark Adler [madler@alumni.caltech.edu](mailto:madler@alumni.caltech.edu)
Overview

This appendix provides information on the formats of each of the downloaded logs from the Local Security Manager (LSM). This includes information on the remote syslog format and High Availability messages contained in the System Log, as well as messages received during the system update process.

- “Log Formats” on page 146
  - “Alert and IPS Block Log Formats” on page 146
  - “Audit Log Format” on page 148
  - “System Log Format” on page 149
- “Remote Syslog Log Format” on page 150
- “High Availability Log Messages” on page 151
- “System Update Status Messages” on page 152
Log Formats

You can download text-only versions of all LSM logs and view them in a browser window or save them in a file. Saved log files can be offloaded to a remote syslog server. In the System Log, the fields displayed in the LSM match the fields in the downloaded log. In the other logs, the fields displayed in the LSM are only a subset of what is available in the downloaded log file.

This section documents all fields available in the downloaded versions of these logs. These field definitions are helpful when reading the downloaded log file. They contain the description of the data so that you can format the desired fields in a reporting program such as Excel or Access, or send them to a remote syslog server.

Delimiters

When you download a log from the LSM, data is formatted using one of the following delimiters:

- **Tab-delimited**: Default Field names do not appear on the tab delimited format.
- **Comma-delimited format (csv)**: Data is separated by commas. The first row of the log file lists the field names.

For both types of delimiters, the sub-fields within the Message field are always tab delimited. If a Message sub-field is not used a tab is inserted to move onto the next sub-field.

Alert and IPS Block Log Formats

An example of a comma delimited Block Log entry follows:

```
1,2008-10-21 17:50:10,INFO,BLK,Block,v5,2,[00000002-0002-0002-0002-000000003671],4,[00000001-0001-0001-0001-000000003671],tcp,0,
123.56.89.87,80,135.91.246.80,2636,1,16,[cc2f252a-1a75-6d00-8dc8-
a34e69992c64],ANY,[cc2f252a-1a75-6d00-8dc8-
a34e69992c64],ANY,1334629410,0149251970,1, ,pt0,0,0,0,0333
```

When opened in an application such as Excel, each comma-delimited item appears in an individual column.

The following table describes the fields included in the Alert Log and IPS Block Log:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seq</td>
<td>Unique sequence number for this log file.</td>
</tr>
<tr>
<td>Entry_time</td>
<td>Date and time of event. YYYY-MM-DD 24H:MI:SS</td>
</tr>
</tbody>
</table>
| Sev | Severity of the alert, from least to most severe:  
  • INFO = for information only  
  • WARN = warning  
  • ERR = error  
  • CRIT = critical |
Table B - 1: Alert and Block Log Formats (Continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comp</td>
<td>Software component that generated the message:</td>
</tr>
<tr>
<td></td>
<td>• ALT = Alert Log</td>
</tr>
<tr>
<td></td>
<td>• BLK = IPS Block Log</td>
</tr>
<tr>
<td>Log</td>
<td>Log in which the message was recorded:</td>
</tr>
<tr>
<td></td>
<td>• Alert = for Alert Log</td>
</tr>
<tr>
<td></td>
<td>• Block = for Block Log</td>
</tr>
<tr>
<td>Vers</td>
<td>Version number of the policy.</td>
</tr>
<tr>
<td>Alert_type</td>
<td>A bit field that identifies a message as traffic threshold, invalid, etc.</td>
</tr>
<tr>
<td>Policy</td>
<td>ID numbers for the policy, enclosed within brackets ([ ]).</td>
</tr>
<tr>
<td></td>
<td>Default policies begin with [00000002-...</td>
</tr>
<tr>
<td>Max_qual_sev</td>
<td>Message severity:</td>
</tr>
<tr>
<td></td>
<td>• 1 = low</td>
</tr>
<tr>
<td></td>
<td>• 2 = minor</td>
</tr>
<tr>
<td></td>
<td>• 3 = major</td>
</tr>
<tr>
<td></td>
<td>• 4 = critical</td>
</tr>
<tr>
<td>Sig</td>
<td>The Signature UUID from the DV, enclosed within brackets ([ ]).</td>
</tr>
<tr>
<td></td>
<td>Default signatures begin with [00000001-...</td>
</tr>
<tr>
<td>Prot</td>
<td>Protocol of the alert.</td>
</tr>
<tr>
<td></td>
<td>Examples: HTTP, IP, TCP, IDP, and ICMP.</td>
</tr>
<tr>
<td>Reserved</td>
<td>Not used.</td>
</tr>
<tr>
<td>Src</td>
<td>Packet's source IP address.</td>
</tr>
<tr>
<td>Src_port</td>
<td>Packet's source port number.</td>
</tr>
<tr>
<td>Dest</td>
<td>Packet's destination IP address.</td>
</tr>
<tr>
<td>Dest_port</td>
<td>Packet's destination port number.</td>
</tr>
<tr>
<td>Packets_delta</td>
<td>The aggregated number of messages received.</td>
</tr>
<tr>
<td>MPHY</td>
<td>The number of the physical port number on which the packet arrived.</td>
</tr>
<tr>
<td>VLAN</td>
<td>The number of the VLAN on which the packet arrived.</td>
</tr>
<tr>
<td>In_sec_zone</td>
<td>The UUID of the security zone on which the packet arrived.</td>
</tr>
<tr>
<td>In_sec_zone_name</td>
<td>The name of the security zone on which the packet arrived.</td>
</tr>
<tr>
<td></td>
<td>Example: ANY</td>
</tr>
<tr>
<td>Out_sec_zone</td>
<td>The UUID of the security zone on which the packet went out.</td>
</tr>
<tr>
<td>Out_sec_zone_name</td>
<td>The name of the security zone on which the packet went out.</td>
</tr>
<tr>
<td></td>
<td>Example: ANY</td>
</tr>
<tr>
<td>Start_sec</td>
<td>Beginning timestamp of the aggregation period, in seconds.</td>
</tr>
</tbody>
</table>
An example of a comma delimited Audit Log entry follows:

```
14,2008-10-21 17:32:34,8,CLI,0.0.0.0,Host,0,0,root00,"Host name changed to ncp88"
```

The following table describes the downloadable format of the Audit Log:

**Table B - 2: Audit Log Format**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seq</td>
<td>Unique sequence number for this log file.</td>
</tr>
<tr>
<td>Entry_time</td>
<td>Date and time of event. YYYY-MM-DD 24H:MI:SS</td>
</tr>
<tr>
<td>Access</td>
<td>The access-level of the user performing the action.</td>
</tr>
<tr>
<td>Type</td>
<td>The interface from which the user logged in.</td>
</tr>
<tr>
<td></td>
<td>• WEB for the LSM</td>
</tr>
<tr>
<td></td>
<td>• CLI for the Command Line Interface</td>
</tr>
<tr>
<td></td>
<td>• SYS for the console</td>
</tr>
<tr>
<td>Address</td>
<td>The IP address from which the user connected to perform the action.</td>
</tr>
<tr>
<td>Cat</td>
<td>The area in which the use performed an action (LOGIN, LOGOUT, and Launch Bar tabs).</td>
</tr>
<tr>
<td>Result</td>
<td>The result of the audited action:</td>
</tr>
<tr>
<td></td>
<td>• 0 = Pass</td>
</tr>
<tr>
<td></td>
<td>• 1 = Fail</td>
</tr>
</tbody>
</table>
**System Log Format**

An example of a comma delimited System Log entry follows:

```
121,2008-10-21 17:49:33,INFO,INT,"System Initialization Complete"
```

The following table describes the downloadable format of the System Log:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seq</td>
<td>Unique sequence number for this log file.</td>
</tr>
<tr>
<td>Entry_time</td>
<td>Date and time of event. YYYY-MM-DD 24H:MI:SS</td>
</tr>
<tr>
<td>Sev</td>
<td>Severity of the alert, from least to most severe:</td>
</tr>
<tr>
<td></td>
<td>• <code>INFO</code> = for information only</td>
</tr>
<tr>
<td></td>
<td>• <code>WARN</code> = warning</td>
</tr>
<tr>
<td></td>
<td>• <code>ERR</code> = error</td>
</tr>
<tr>
<td></td>
<td>• <code>CRIT</code> = critical</td>
</tr>
<tr>
<td>Comp</td>
<td>Software component that generated the message.</td>
</tr>
<tr>
<td></td>
<td><strong>Examples:</strong> SYS, UDM, and HTP</td>
</tr>
<tr>
<td>Message</td>
<td>The message text associated with the event.</td>
</tr>
<tr>
<td></td>
<td>For a list of High Availability messages, see section &quot;High Availability</td>
</tr>
<tr>
<td></td>
<td>Log Messages&quot; on page 151.</td>
</tr>
</tbody>
</table>
Remote Syslog Log Format

The remote syslog format for the Alert and Block Logs is described in this section.

**Note:** For the System and Audit Logs, there is no specific format for the remote syslog. For these logs, the downloaded file is sent directly to the remote syslog server as a straight data dump without any manipulation of the data.

The following is an example of packet data sent to a collector. Note that collectors may display the header portion of the stream differently. In this example, the header follows the standard syslog format.

```
192.168.65.22,265155,1,Permit,Minor,00000002-0002-0002-0002-
0000000161,"0161: ICMP: Redirect Undefined Code","0161: ICMP:
Redirect Undefined Code",icmp,"",90.138.157.173,0,90.138.157.175,0,
20081024T213932+0360,1,"",0,ANY-ANY
```

Using the previous log entry as the example, the message is as follows:

```
ALT,v5,20081024T213932+0360,irobot/
192.168.65.22,265155,1,Permit,Minor,00000002-0002-0002-0002-
0000000161,"0161: ICMP: Redirect Undefined Code","0161: ICMP:
Redirect Undefined Code",icmp,"",90.138.157.173,0,90.138.157.175,0,
20081024T213932+0360,1,"",0,ANY-ANY
```

The character located between each field is the configured delimiter. In this case, the delimiter is a comma. The following table details the fields and their descriptions.

**Table B - 4: Remote Syslog Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log-type; ALT = alert, BLK = block</td>
</tr>
<tr>
<td>2</td>
<td>Version of this message format</td>
</tr>
<tr>
<td>3</td>
<td>ISO 8601 Date-Time-TZ when this alert was generated</td>
</tr>
<tr>
<td>4</td>
<td>Hostname/IP address that generated the alert. The hostname is enclosed in quotes if the name contains non-alphanumeric characters, such as spaces.</td>
</tr>
<tr>
<td>5</td>
<td>Sequence ID</td>
</tr>
<tr>
<td>6</td>
<td>(reserved)</td>
</tr>
<tr>
<td>7</td>
<td>Action performed (“Block” or “Permit”)</td>
</tr>
<tr>
<td>8</td>
<td>Severity (“Low”, “Minor”, “Major”, or “Critical”)</td>
</tr>
<tr>
<td>9</td>
<td>Policy UUID</td>
</tr>
<tr>
<td>10</td>
<td>Policy Name</td>
</tr>
<tr>
<td>11</td>
<td>Signature Name</td>
</tr>
<tr>
<td>12</td>
<td>Protocol name (“icmp”, “udp”, “tcp”, or “unknown”)</td>
</tr>
</tbody>
</table>
High Availability Log Messages

The High Availability mechanism records the following messages to the System Log. For details on the System Log, see “System Log Format” on page 149.

Table B - 5: High Availability Log Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Fallback (Intrinsic HA) cause: failed manually</td>
<td>Critical</td>
<td>User has manually placed the IPS device into HA from the LSM (System &gt; HA) or the CLI.</td>
</tr>
<tr>
<td>Layer 2 Fallback (Intrinsic HA) cause: none (cleared manually)</td>
<td>Informational</td>
<td>User has manually taken the IPS device out of HA via the LSM or the CLI.</td>
</tr>
<tr>
<td>Layer 2 Fallback (Intrinsic HA) cause:</td>
<td>Critical</td>
<td>When the IPS device goes into HA because of an internal system failure, an error message indicates the cause of the failure. Use this information when you contact TippingPoint Technical Support for assistance.</td>
</tr>
<tr>
<td>• suspended task</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• memory issue</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• hardware breakpoint</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• TSE failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Software watchdog timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• watchdog timeout</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Threshold Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• OAM Fault Recovery</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
System Update Status Messages

The LSM provides update status on the progress of the update. The messages include “<Update State>:<qualifier>“. The <Update State> indicates the state of the update. The <qualifier> provides information about the state. The following table details the messages that display on the LCD screen during an update of the TOS:

Table B - 6: IPS Update States

<table>
<thead>
<tr>
<th>Update State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ready</td>
<td>Device is ready for an update.</td>
</tr>
<tr>
<td>Updating</td>
<td>Device is in the process of updating.</td>
</tr>
<tr>
<td>UpdateCommitting</td>
<td>Device has rebooted and is processing the final update steps.</td>
</tr>
<tr>
<td>UpdateFailure</td>
<td>Device failed update. The screen displays the reason.</td>
</tr>
<tr>
<td>Rollback</td>
<td>Device is in the process of rollback.</td>
</tr>
<tr>
<td>RollbackCommitting</td>
<td>Device has rebooted and is processing the final rollback steps.</td>
</tr>
<tr>
<td>RollbackFailure</td>
<td>Device failed rollback. The screen displays the reason.</td>
</tr>
<tr>
<td>Failsafe</td>
<td>Device was unable to load a valid image and is running a scaled-back image.</td>
</tr>
</tbody>
</table>

If an error occurs, the information changes. The state displays as “UpdateFailure:<state>.“ where <state> is one of the listed states in Table B - 6. The listed state displays a qualifier and message regarding the state. The following table details the qualifier and messages:

Table B - 7: IPS Update Failure Messages

<table>
<thead>
<tr>
<th>Update Failure Qualifier</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>OK</td>
<td>Normal operation, no errors</td>
</tr>
<tr>
<td>InvalidUpdateState</td>
<td>Current action is restricted while device is in this state. Fix problem and reset Update State.</td>
</tr>
<tr>
<td>InvalidLocation</td>
<td>Package file not found at that location.</td>
</tr>
<tr>
<td>RebootDuringUpdate</td>
<td>Device was rebooted during update. Check system log for recommendations.</td>
</tr>
<tr>
<td>TarChecksumError</td>
<td>Checksum error when extracting the archive: Corrupted package.</td>
</tr>
<tr>
<td>TarExractError</td>
<td>File system error when extracting the archive.</td>
</tr>
<tr>
<td>ArchiveCreateFailure</td>
<td>File system error creating rollback archive.</td>
</tr>
<tr>
<td>SystemError</td>
<td>General error during update.</td>
</tr>
<tr>
<td>WrongPlatformType</td>
<td>Package is for a different platform. Make sure you have correct TippingPoint supplied IPS package.</td>
</tr>
</tbody>
</table>
### Table B - 7: IPS Update Failure Messages (Continued)

<table>
<thead>
<tr>
<th>Update Failure Qualifier</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>PackageReadError</td>
<td>General error while reading package. Possible truncated or corrupted package; download new package from TMC and retry update.</td>
</tr>
<tr>
<td>WrongPackageType</td>
<td>Package is of unknown type, not an OS or DV package. Make sure you have correct TippingPoint supplied IPS package.</td>
</tr>
<tr>
<td>NotEnoughFreeSpace</td>
<td>Not enough available disk space. Remove older installed images.</td>
</tr>
<tr>
<td>UnsignedPackage</td>
<td>Package does not have proper TippingPoint digital signature.</td>
</tr>
<tr>
<td>MemoryError</td>
<td>Memory error when installing package. Reboot may be necessary.</td>
</tr>
<tr>
<td>BadCertificate</td>
<td>Package does not have proper TippingPoint digital certificate.</td>
</tr>
<tr>
<td>DowngradeRevisionNotSupported</td>
<td>Using update to install some older versions is not supported.</td>
</tr>
<tr>
<td>PackageOpenError</td>
<td>Unable to open package. Make sure you have a correct TippingPoint-supplied IPS package.</td>
</tr>
<tr>
<td>CannotUpdateDVWhenTSEIsBusy</td>
<td>Unable to update Threat Suppression Engine packages while the system is busy reloading filters. Retry operation at a later time.</td>
</tr>
</tbody>
</table>
Overview

This chapter describes how to configure the TippingPoint system for management by Network Management Systems (NMS), a common term for SNMP management systems. It includes the following sections:

- “Enabling NMS Communication” on page 155
- “Using the IPS MIBs” on page 156
- “Using HP OpenView With IPS MIBs” on page 158

Note: The MIB files are available in a .zip file and can be downloaded from the TippingPoint TMC at https://tmc.tippingpoint.com.

Enabling NMS Communication

Before you begin, you must enable NMS communication on the IPS. In the Command Line Interface (CLI), use the `conf t nms` command to configure the SNMP trap port number (default 162), and the community string. Once you have entered this information, your NMS can manage TippingPoint IPS devices. For detailed information about the `conf t nms` command, refer to the TippingPoint Command Line Interface Reference.

If the IPS does not permit you to configure the NMS settings, the device may be under SMS management. Use the `conf t no sms` command to disable SMS management before continuing.
Using the IPS MIBs

This section describes the MIB files available for the IPS. You can download a .zip file containing the complete MIB files from the TMC at https://tmc.tippingpoint.com.

**TIPPINGPOINT-REG-MIB**

- **Description**: Defines the OID sub-tree assigned to TippingPoint by the Internet Assigned Numbers Agency (IANA), as well as sub-trees for registered modules, object and event definitions, agent profiles, management application requirements, and experimental definitions.

  **Note**: This MIB file must be loaded before you load any other TippingPoint MIB files.

**TPT-COMPACT-FLASH**

- **Description**: Defines the status and operating mode of the compact flash card.

**TPT-HEALTH**

- **Description**: Indicates the health status of the IPS. Features monitored temperatures, fan speeds, and voltage levels.

**TPT-HIGH-AVAIL**

- **Description**: Defines the conditions and actions for Intrinsic Network HA, Transparent Network HA, and Zero-Power HA, and also offers information about the current fault state of the device.

**TPT-HOST**

- **Description**: Defines the IPS host information, the default gateway address, and indicates whether the device is currently configured for service access.

**TPT-LICENSE**

- **Description**: Support for TippingPoint license packages, including TOS, Digital Vaccine, IP Reputation, and other services.

**TPT-MISC-NOTIFY**

- **Description**: Notifications for logs and other features.

**TPT-MULTIDV**

- **Description**: Manages the MultiDV feature.
TPT-NPSTATS

- **Description**: Lists network processor tier statistics.

TPT-POLICY

- **Description**: Defines variable definitions, Digital Vaccine information, reports, policy information, and policy notification information.

TPT-PORT-CONFIG

- **Description**: Defines port configuration settings.

TPT-RESOURCE

- **Description**: Describes memory, power supply, temperature, and voltage information for the device.

TPT-SMSMIBS

- **Description**: Defines interactions between the IPS and the SMS.

TPT-SMS-TRAP-MIB

- **Description**: Describes notifications sent to and from an SMS device.

TPT-TPA-HARDWARE

- **Description**: Describes the device hardware and its components, including ports, chassis, fans, and power supplies.

TPT-TPAMIBS

- **Description**: Defines additional MIB sub-trees.

TPT-TRAFFIC

- **Description**: Defines traffic rate-limiting information.

TPT-TSE

- **Description**: Defines TSE settings, including adaptive filtering.
Using HP OpenView With IPS MIBs

HP OpenView is a well-known commercial network management system. Much of this information can be transposed onto other network management systems.

This section focuses on adding enterprise MIB monitoring and reporting to HP OpenView. The examples in this section were created on HP OpenView 7.0.1 running on Windows XP Professional Service Pack 1.

Note: This book assumes that you have already installed HP OpenView. Refer to the OpenView documentation for more information about that product.

This section includes the following:

- “Loading TippingPoint Enterprise MIBs” on page 158
- “MIB Application Builder” on page 158
- “Discovering the IPS” on page 159
- “Creating Graphs with Application Builder” on page 160

Loading TippingPoint Enterprise MIBs

Before you begin, you must configure OpenView to understand the TippingPoint Enterprise MIBs.

1. In the OpenView Root Map, select the Options menu.
2. Select Load/Unload MIBs: SNMP.
3. Load TIPPINGPOINT-REG-MIB.
4. Load the remaining TPT MIBs in any order. OpenView may prompt you when loading the MIBs regarding adding a macro definition. This is normal behavior, and you should accept the MIB.

MIB Application Builder

OpenView includes a tool called MIB Application Builder that allows you to build custom applications that retrieve data using SNMP and to retrieve any information stored in a MIB.

2. Select Edit => New item. The application prompts you with three fields: Application ID, Application Type and Application Title.
   A. Enter 111 for the Application ID.
   B. Leave the Application Type as Form.
   C. Enter an Application Title.
3. Select the MIB Objects that have the information that you want to view.

4. Click Next.
The MIB Application Builder / Add MIB Objects screen displays.

5. In the navigation tree, locate iso.org.dod.internet.private.enterprises. You are now at the start of the IPS MIBs.

6. In the tree, select the variables that you want to monitor and click Add. Click Close to return to the previous screen.

7. Depending on how you added the objects, you may need to reorder them. You can reorder the variables by using the up and down arrows in the New MIB Application - Display Fields form.

8. Click Next to continue to the New MIB Application - NMN Integration dialog screen.

9. Enter TippingPoint after Configuration->. The line should appear as Configuration->TippingPoint under Menu Location. This creates a menu item under the Configuration menu on the main screen.

10. You can select an object on the map. Select Configuration from the menu and retrieve the information you created if the device is a TippingPoint device.

11. Close the MIB Application Builder dialog box.

Discovering the IPS

By default, OpenView assumes that you would rather automatically discover devices as they arrive on the network. This form of discovery can be a slow process and may not display devices for days (depending on the size of your network). To expedite that process, you use the loadhosts command.

1. Open your text editor and create a file named hosts.

2. In the file, enter the IP address of your IPS and the hostname. This format is similar to the UNIX /etc/hosts file format. For example, you might enter the following information:

3. 192.168.65.20nds10

4. Save the file and open a command shell.

5. Run the loadhosts command on the file. The command takes the network mask and the file as arguments. For example:

   loadhosts -m 255.255.255.0 hosts

After you run the loadhosts command, the device is now discovered by OpenView. When you open the Internet icon on your OpenView map, a green square displays. This icon should be your device or devices. Select this icon and choose Configuration from the menu bar to view the device.

OpenView has a number of built-in applications that can retrieve data from standard MIBs. For example, when you open the IPS configuration, all of the Ethernet interfaces associated with that device are displayed. When you right-click on the interface and choose Interface Properties. Information for that interface is displayed.
Creating Graphs with Application Builder

You can create an application to graph the data with the MIB Application Builder tool.

1. Select the Application Builder from the **Options** menu.
2. Open your existing applications and double-click to edit.
3. Change the **Application Type** from a **Form** to a **Graph**.
4. Set “10” as the **Poll Interval** and “abc” as the **Y-axis** label. You can change these settings to fit your needs.
5. To generate the graph for your device, select the IPS green square. Choose **TippingPoint** from the **Configuration** menu. A graph displays for the device. Allow the graph to run about 30 seconds to begin trending the data.
Glossary

**action set**
An integral part of an attack or peer-to-peer filter, action sets determine what the IPS device does when a packet triggers a filter. An action set can contain more than one action, and can contain more than one type of action. The types of action that can be specified include the following:

- **Flow Control actions** — determines where a packet is sent after it is inspected. *Permit* allows a packet to reach its intended destination. *Block* discards a packet. A block action can also be configured to *quarantine* the host and/or perform a *TCP reset*. *Rate limit* action enables you to define the maximum bandwidth available for the traffic stream.

- **Packet Trace action** — captures all or part of a suspicious packet for analysis depending on how the packet trace options are configured.

The system comes with a set of default action sets that are applied to groups of filters based on a category setting recommended by TippingPoint’s Threat Management Center. The default action sets can be customized for individual filters or groups of filters. You can also create new action sets.

**Adaptive Filter Configuration**
This function allows you to configure the IPS to protect against potential adverse affects of a defective filter. When Adaptive Configuration is turned on and the network is experiencing heavy loads, the IPS will automatically disable any filter that may be causing the congestion to prevent the device from entering High Availability mode and going offline. AFC settings are set to either Auto or Manual for the entire IPS. The default is Auto which means that AFC is on. AFC can also be turned on or off for specific filters.

**aggregation period**
The length of time during which multiple instances of a specific attack can occur before notification is sent to a contact.
**Application Protection**

Category of filters that defend against known exploits and exploits that may take advantage of known vulnerabilities targeting applications and operating systems. This filter type includes the following sub-categories: Exploits, Identity Theft, Reconnaissance (includes Port Scan/Host Sweep filters), Security Policy, Spyware, Virus, and Vulnerabilities. These filters detect specific recognition data to recognize an attempted attack and take specific courses of action that you define when an attempt is detected.

**attack filter package**

See Digital Vaccine Package.

**attack traffic**

Packets traversing a network that match at least one Application Protection filter.

**asymmetric network configuration**

Out of the box, the IPS will identify flows in asymmetric mode – meaning the IPS only needs to see either the transmit or the receive side of a TCP connection (not both). If you want to use DDoS filters on your IPS device, you must disable asymmetric mode.

**category**

Digital Vaccine filters are organized into three main categories based on the type of protection provided: Application Protection, Infrastructure Protection, and Performance Protection. These categories are used to organize and locate filters in the LSM web application.

**category settings**

Category settings are used to assign global configuration settings to filters within a category. For example, a Vulnerability filter responds to attack traffic based on the category settings for the Application Protection category while a Network Equipment filter would respond based on the category settings for the Infrastructure Protection category. Users can edit individual filters within a sub-category to override the category settings for the filter. Category settings consist of the following global parameters:

- **State** — determines whether filters within the sub-category are enabled or disabled. If a category is disabled, all filters in the Category are disabled.
- **Action Set** — determines the action set that filters within a Category will execute when a filter match occurs. If the Recommended action set is configured, filters within the category are configured with the settings recommended by the Digital Vaccine team. If required, you can override the category setting on individual filters by editing the filter to define custom settings.

**Certificate Authority (CA)**

A trusted third-party entity which issues digital certificates for use by other parties.

**Certificate Revocation List (CRL)**

A list of serial numbers for certificates that are no longer valid.
**Classless Inter-Domain Routing (CIDR)**

An address format similar to an IP address except that it is followed by a slash (/) and a specified number of bits. The number of bits indicates the significant bits in the address. In the following example, the IP source address of a packet must match all 32 bits of the IP address specified:

10.3.4.5/32

**Custom Shield Writer (CSW)**

An optional, stand-alone, TippingPoint application to write custom filters that can be imported for use on IPS and SMS devices.

**DER**

Stands for Distinguished Encoding Rules. DER is a method for encoding X.509 certificates to be digitally signed or to have their signatures verified. DER files are binary files.

**Digital Vaccine Filters**

Digital Vaccine Filters block attacks and other malicious traffic from the network. Filters come with a set of recommended (default) settings which specify the filter status (enabled or disabled), the type of action to be taken when the filter is triggered (action set defined to permit or block traffic and/or send a notification) and the Adaptive Filter Configuration setting (on or off). Users can accept the default settings, or override them based on network security needs. Digital Vaccine filters are categorized in the following groups: Application Protection and Performance Protection.

Digital Vaccine filters are created by the TippingPoint Threat Management team that monitors global network security threats and continually develops new attack filters which are automatically distributed to pre-emptively protect against the exploit of new and zero day vulnerabilities. Updates are distributed using Digital Vaccine Packages.

**Digital Vaccine Package**

Downloadable software update that includes Digital Vaccine filters that provide the most current IPS protection for your network. The Digital Vaccine Package is available from the TippingPoint Threat Management Center (TMC) (https://tmc.tippingpoint.com/TMC). Devices can also be configured to download and install the Digital Vaccine packages automatically.

**DDoS filters**

Group of infrastructure protection filters that detect DDoS (distributed denial-of-service) attacks which flood a network with requests, including traditional SYN floods, DNS request floods against nameservers, and attempts to use protected systems as reflectors or amplifiers in attacks against third parties. These filters detect direct flood attacks and attacks hidden within larger packets and requests. DDoS filters include the following filters: SYN Proxy, Connection Flood, and CPS Flood filters.

**Exploit filters**

Filters that protect software from malicious attacks across a network by detecting and blocking the request. Exploits are attacks against a network using weaknesses in software such as operating systems and applications. These attacks usually take the form of intrusion attempts and attempts to destroy or capture data. These filters are part of the Application Protection filter category.
filter
Policy consisting of rules and conditions used to detect and manage malicious traffic on a network. Each filter includes an action set with instructions for managing data when the filter is triggered and category settings. The LSM includes various types of filters, including Digital Vaccine filters in the Performance Protection, Application Protection categories along with traffic management, traffic threshold, and DDoS filters.

High Availability
High Availability is a system configuration setting that helps guarantee that your network traffic always flows at wire speeds in the event of any internal hardware or software failure on the IPS devices. The IPS device has three mechanisms for High Availability configuration: Intrinsic Network HA, Transparent HA, and Zero-Power HA.

Identity Theft filters
Filters protect end users from Phishing attacks by detecting and blocking connections to known Phish sites and attacks. A Phishing Attack is typically an email or web site which has been spoofed to appear as if it is from a well known financial or transaction institution. The attacks are usually geared to obtain account information from the end user. These filters are part of the Application Protection filter category.

IM filters
IM filters detect and control traffic from Instant Messaging applications such as Yahoo Messenger or MSN Messenger, chat, file transfer and photo sharing. These filters can be used to block the operation of the Instant Messaging application. Many of the IM filters can also be used to rate limit traffic from IM applications. These filters are part of the Performance Protection filter category.

Infrastructure Protection
Category of filter types that protect network bandwidth and network infrastructure elements such as routers and firewalls from attack using a combination of traffic normalization, DDoS protection, and application, protocol, and network equipment protection. These filters include DDoS, network equipment protection, and traffic normalization filters.

Intrinsic Network High Availability
Intrinsic Network HA determines how the IPS device manages traffic on each segment in the event of a system failure. When the system fails, the device goes into Layer-2 Fallback mode and either permits or blocks all traffic on each segment, depending on the Layer-2 Fallback action setting for the segment. When the device is in Layer-2 Fallback mode, any traffic allowed through the device will not be inspected; it simply passes through the device.

Intrusion Prevention System (IPS)
The first active network-defense system that provides true intrusion prevention. Based on breakthrough high-speed security processors, TippingPoint becomes part of the network-infrastructure and scours networks at high speed to identify and act upon malicious traffic. Unlike intrusion detection systems, TippingPoint continually cleanses Internet and Intranet traffic, identifying and preventing attacks before damage to critical resources occurs, ensuring network integrity and ultimately improving return on investment.
Layer-2 Fallback

For IPS devices configured for Intrinsic Network High Availability, Layer-2 fallback mode refers to the state of the device when Intrinsic Network HA is triggered (the device fails). When the device is in Layer-2 Fallback mode, all traffic on each segment is either permitted or blocked, depending on the Layer-2 Fallback action setting for the segment. When the device is in Layer-2 Fallback mode, any traffic allowed through the device will not be inspected.

Local Security Manager (LSM)

A web-based management application that provides on-the-box administration, configuration, and reporting for a single Intrusion Prevention System (IPS).

Network Equipment filters

Filters that detect and block the malicious attacks that target equipment accessible through a network. Network attacks can broadly or specifically seek access and data to corrupt on a network. These filters are part of the Infrastructure Protection filter category.

notification contacts

Recipients of alert messages. These contacts receive an email alert when a filter with the proper notification contacts settings triggers. Contacts include staff with email accounts and the SMS application. You can configure notification contacts from the IPS > Action Sets menu item.

packet trace

An option available for action sets, this setting allows you to capture all or part of a suspicious packet for analysis. You can set the packet trace priority and packet trace verbosity for action sets.

Performance Protection

Category of filter types that allow key applications to have prioritized access to bandwidth ensuring that mission critical applications have adequate performance during times of high congestion. These filters include misuse and abuse, IP, and congestion/mitigation filters.

physical segment

A physical segment comprises a group of hosts protected by IPS through a pair of physical ports on an IPS device. You can configure traffic management and DDoS filters using physical segments.

Port Scan/Host Sweep filters

Filters that perform port scans and host sweeps to prevent any malicious code, attacks, and exceeded threshold limits for traffic. Each filter scans a specific type of port and protocol to block attacks against ports and hosts. These filters are part of the Application Protection filter category.
PEM

PEM stands for Privacy Enhanced Mail. PEM X.509 certificates are Base64-encoded DER certificates that may contain certificates or private keys. The encoding output is enclosed between the following lines:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

P2P filters

Filters that use the same algorithms as attack filters, but which block peer-to-peer protocol traffic. These protocols are primarily used to share music and video files. They essentially turn a personal computer into a file server which makes its resources as well as those of its host network available to the peer-to-peer community. These filters are part of the Performance Protection filter category.

Quarantine

Quarantine allows the IPS system to block packets based on the IP addresses in a packet that triggers a filter. When a filter with a quarantine option triggers, the device installs two blocks: one for the flow (as is normally done with Block actions) and another for the quarantined IP address. Quarantine is a configurable option available on Action Sets. Setting up quarantine on a filter requires assigning a Quarantine action set to the filter. For details, see "Quarantine actions" on page 52.

rate limit

Setting in an action set that defines a maximum bandwidth that can be used by traffic that matches filters assigned to that action set. Incoming traffic in excess of this bandwidth is dropped. If two or more filters use the same rate limiting action set, then all packets matching these filters share the bandwidth.

Reconnaissance filters

Reconnaissance filters monitor traffic for events that indicate network activity usually associated with common information gathering techniques used by attackers to launch more sophisticated attacks. These attacks search through your network using various methods to locate vulnerabilities. After the attack has gathered data by probing your system and scanning your network, it continues with pointed attacks against those vulnerabilities. Reconnaissance filters look for these patterns and alert either the LSM or the SMS when an attack is detected. Port Scan/Host Sweep filters (see page 165) filters are included in this category. These filters are part of the Application Protection filter category.

Security Management System (SMS)

A Linux management server and Java-based client application for managing multiple IPS devices. It provides coordination across your IPS devices for administration, configuration, and monitoring, attack filter customization, centralized distribution of upgrades, and enterprise-wide reporting and trend analysis.

Security Profiles

A security profile is used to set up Digital Vaccine filters to monitor traffic passing on one or more virtual segments. The profile consists of category settings for the DV filters along with any user-
defined filter overrides and IP address limits/exceptions. After a security profile is created, the IPS will begin monitoring traffic on the segments included in the profile using the specified the filter settings.

**Security Policy**

Security Policy refers to all of the mechanisms available on the IPS device to protect and manage network traffic including traffic management profiles and security profiles (Digital Vaccine Filters), DDoS and Traffic Threshold filters. These profiles and filters are configured based on your network deployment and operational policy.

**SNMP Server**

Provides access to interface counters and other statistics, configuration data, and general system information via the Simple Network Management Protocol (SNMP). The SNMP server must be enabled to use SMS management or to allow NMS access.

**spyware filters**

Spyware filters detect and block downloads, communications and pop-ups sent via spyware.

**Streaming Media filters**

Streaming Media filters detect and control traffic from Streaming Media applications that deliver audio and video content utilizing IP protocols, typically UDP. Because these streaming media applications demand high bandwidth, the use of these applications can have a large negative impact on network performance. These filters can be used to block the operation of the Instant Messaging application. Many of the IM filters can also be used to rate limit traffic from IM applications. These filters are part of the Performance Protection (see page 165) filter category.

**Traffic Management filters**

Filters that react to traffic based on a limited set of parameters including the source IP address, destination IP address, port, protocol, or other defined values. Users can create and configure traffic management filters from the LSM or CLI interface on the IPS device. Traffic management filters can only be applied to physical segments; you cannot apply traffic management filters to traffic based on VLAN ID.

**Traffic Normalization filters**

Filters that block network traffic when the traffic is considered malicious. These filters allow you to set alerts to trigger when the system recognizes this traffic. Traffic pattern filters alert when network traffic varies from normal. These filters are part of the filter category.

**transparent network high availability**

Transparent Network HA is a software/hardware solution that requires installing two IPS devices in a redundant network configuration. The devices are configured so that if one device experiences failure, the network traffic can be routed to the other device with no interruption.

**Threat Management Center (TMC)**

A TippingPoint service center that monitors sensors around the world for the latest attack information and builds and distributes up-to-date filter protection via the Digital Vaccine package. The TMC is available at the following URL: [https://tmc.tippingpoint.com](https://tmc.tippingpoint.com)
**Threat Suppression Engine (TSE)**

Blend of Application-Specific Integrated Circuits (ASICs) and network processors that detect threats and anomalies in your network traffic. The TSE scans and reacts to malicious attacks or anomalous traffic based on the configuration of the IPS security profiles and traffic management and traffic thresholds filters using the latest Digital Vaccine package updates.

**virtual port**

A virtual port is a software-defined port that includes a physical port and one or more VLAN IDs. A virtual port is used to apply IPS filters to traffic based on the incoming and outgoing port and VLAN ID. An IPS device has a virtual port defined for each physical port on the device by default. These default ports are used to apply security policy to all traffic on the specified port with any VLAN ID. If your network environment does not require security policy based on VLANs, you can use the default virtual ports to configure the security profiles, traffic threshold and traffic management, and DDoS filters. To apply IPS security policy based on specific VLAN IDs, you can create virtual ports based on your network requirements.

**Table A - 1: Virtual Port**

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port1/ANY</td>
<td>virtual port that encompasses all traffic on Port 1 with any VLAN ID.</td>
</tr>
<tr>
<td>ANY/VLAN1</td>
<td>virtual port that encompasses all VLAN1 traffic on any port.</td>
</tr>
<tr>
<td>Port 1,2/VLAN 6-10</td>
<td>virtual port that encompasses any traffic on ports 1 and 2 from VLAN 6, 7, 8, 9, and 10</td>
</tr>
</tbody>
</table>

**Virus filters**

Virus filters detect and block events triggered by viruses, worms, Trojans, backdoors, and other blended malware threats. These filters are part of the Application Protection (see page 162) filter category.

**virtual segment**

A virtual segment comprises a group of hosts protected through a pair of virtual ports on an IPS device. A virtual segment consists of a pair of physical ports and VLAN IDs Virtual segments enable you to logically segment your networks so that the IPS device can monitor and manage traffic based on port and VLAN ID.

**Vulnerabilities filters**

Filters that detect any attempt to exploit a vulnerability in any application, operating system, or networked hardware device. These filters determine whether a vulnerability exists based on traffic requests and reaction by services. These filters are part of the Application Protection (see page 162) filter category.
X.509

An international standard for what should be included in a digital certificate. Specifies standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.
Index

A
access level user 132
action sets about 10
Action Sets page 50
adding notification contact 57
adding remote system log contact 56
Block 51
Block + Notify 51
Block + Notify + Trace 51
creating 53
deleting notification contact 57
editing 53
notification contacts 50
packet trace 50
Permit + Notify 51
Permit + Notify + Trace 51
quarantine 52, 166
rate limit 52
Recommended 51
trust 51
adaptive filtering
Adaptive Filter Reports page 89
configuration 61
disabling 89
global settings 90
administrator 132
aggregation period 55, 57
alert aggregation 55
alert log 65
architecture 2
audit log 67
authentication 131
Auto Refresh 19, 136

C
category settings editing 34
ing for a filter group 34
ing for individual filters 36
remote system log 56
connection table timeout 60
critical thresholds 110

D
DDoS 37, 163
Digital Vaccine
about 29
automatic update 97
configuring filters 29
filters 29
managing filters 96
manual update 98
packages 97
updating filters 97
version 21
viewing 30
disk usage
default threshold 110
documentation xiii

E
e-mail
adding contact 57
Email Server page 111
failure 111
setting server 111
testing 111
threshold 111

F
filters
adding to a security profiles 33
Application Protection 7
category settings 36
creating traffic management 41
custom settings 34
default settings 33
Digital Vaccine 11, 29
edit settings 36
editing category settings 34
exceptions 13
filter groups 34
Infrastructure Protection 7
limits 13
list 32
overrides 34
overview 29
Performance Protection 7
resetting 40
searching 30
Traffic Management 11
viewing 30, 33

G
global exceptions 39
global limits 39
guide
conventions xii
overview xi
target audience xi

H
health
Auto Refresh option 136
default disk and memory thresholds 110
monitor 81
performance 82
resetting default disk and memory thresholds 110
system 20, 80
Index

high availability
  configuring 109
  High Availability page 108
Intrinsics Network HA (INHA) 6, 83, 84, 108, 117, 118
Link-Down Synchronization 116, 117, 118
Transparent HA 83, 85
Transparent Network HA (TNHA) 6, 109
Zero Power HA (ZPHA) 6, 83, 85, 109
HP OpenView 158

I
inspection bypass rules 15
Intrusion Prevention System (IPS)
  client 5
  devices 4
  IPS filtering 23
  IPS Preferences page 59
  IPS Services page 58
IPv4 36, 39, 112
IPv6 14, 36, 39, 112

L
level
  user access 132
logging in 15
logs
  alert 65
  audit 67
  Auto Refresh option 136
  block 66
  downloading 70
  formats 146
  logging mode 61
  overview 64
  rate limit reports 87
  resetting 70
  searching 71
  summary 22
  system 67
  viewing 69
LSM
  Auto Refresh 136
  content and functionality 19
  interface 17
  logging in 15
  menu bar 18
  navigation 9
  navigation pane 18
  security 15
  System Summary 20

M
Managed Streams page 72
management console
  configuring 55
  contact 55
management port
  configuration 103
Management Port page 101
Management Routing page 103
memory usage threshold 110
MBs
  IPS 156
  loading 158
  using 158
model number 21
Monitor page 81

N
named networks
  adding 113
  Named networks page 112
network 115
Network Port
  configuration parameters 119
  disable 120
  overview, auto-negotiate 118
  restart 120
  troubleshoot link-down errors 121
NMS
  about 106
  configuring 107
  with MBs 155
Notification Contacts
  creating 54
  email failure 111
  notification contacts 111

O
operator 132

P
packet statistics 21
Performance page 82
Permit + Notify 51
Permit + Notify + Trace 51
Port Health page 83
ports
  adding 58
  configuration 58, 120
  creating virtual ports 123
  deleting 59
  disabling 120
  editing virtual ports 124
  errors 121
  health 83
  Network Ports page 118
  restarting 120
  Virtual Ports page 121
preferences
  general user 136
  IPS 59
  Preferences page 136
  setting 137
  setting automatic page refresh 136
  TOS user 136
product code 21
product specification 21

Q
quarantine 52, 72, 77, 166
quarantined addresses
  flushing 78
  forcing 77
  searching 77

R
rate limit
  action set 52
  reports 87
rate-limited streams
  about 72, 75
  flushing 76
  searching 76
reboot 21, 102
refresh 19
remote syslog
  configuring 68
  contact 56
  format 150
  setting servers 112
  Syslog Servers page 112
reports
  adaptive filter 89
  rate limit 87
  Top Ten 87
  traffic 88
reputation filter
  creating 38, 48
  deleting 49
  editing 38, 49
  settings 38
Index

reputation groups
  about 47
  creating 48
ReputationDV 48
role 132
rollback messages 152
routing options 103

S
screen refresh 19
Security Level
  default setting, changing 136
  username and password requirements 136
Security Management System (SMS)
  about 106
  client 3
  components 2
  configuring 107
  device under control of 106
  disabling 108
  enabling 108
  server 3
security precautions 15
security profiles
  adding filters 33
  applying to traffic 27
  configuring exceptions 39
  configuring limits 39
  creating 28
  Digital Vaccine filters 29
  editing 28
  examples 27
  Security Profiles page 24
  with traffic management filter 42
segments
  configuration 117
  configuration parameters 117
  configuring 118
  overview 116
  Segment Configuration page 116
SNMP
  adding contact 57
  server 106, 107
software update
  states, messages 152
user
  role 132
  users
    access level 132
    changing passwords 135
    creating accounts 134
    preferences 136
    setting preferences 137
    User List page 132
    username security requirements 136
    valid username and password 136

T
technical support xiii
Threat Management Center (TMC) 7
Threat Suppression Engine
  about 6
  configuration parameters 60
  configuring 60
  description of 10
thresholds
  critical 110
  disk usage 110
  memory 110
  setting 110
  Thresholds page 110
throughput 82
time options
  internal clock 104
  SNTP server 105
  Time Options page 104
time zones 105
TippingPoint architecture 2
TOS software
  managing 92
  updating 93
  version 21
traffic capture
  about 128
  expressions 129
  starting 129
traffic management filters
  configuring 46
traffic management profiles
  creating 43
  editing 44
  parameters 45, 46
  Traffic Management Profiles page 41
  with security profiles 42
traffic reports 88
trust 51, 72

U
update
  states, messages 152
Update page 92
user
  role 132

V
virtual ports
  creating 123
  editing 124
  managing 121
  Virtual Ports page 121
virtual segments
  about 124
  creating 125
  deleting 125
  VLAN translation 126, 127

W
wildcards 36, 39

X
X.509 certificates
  about 138
  CA Certificates 138
  CRL Certificates 138
  importing 138